NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MODELING THE EFFECTS OF CYBER OPERATIONS ON KINETIC BATTLES

by

Fatih Yildiz

June 2014

Thesis Advisor	David Alderson
Co-Advisor	Donald P. Gaver
Second Reader	Patricia Jacobs

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE MODELING THE EFFECTS OF CYBER OPERATIONS ON KINETIC BATTLES		**5. FUNDING NUMBERS**	
6. AUTHOR Fatih Yildiz			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This thesis considers the effects of cyber operations on kinetic warfare, by exploring and building on two recently proposed extensions to traditional Lanchester models of combat. In one model, we consider instantaneous changes to kinetic fighting capability resulting, for example, from the disruption or restoration of communications or other supporting cyber systems. Such changes create discontinuous shocks in the overall combat dynamics and can dramatically affect the outcome of a battle. In the second model, we represent cyber operations as a continuous process of degradation and recovery in fighting capability based on the dynamics of epidemic spread. By using analytical and numerical approaches, we obtain insights about the effect of cyber operations on battle duration and attrition, how cyber operations can affect victory conditions, and tradeoffs in the allocation of limited resources to cyber operations and kinetic operations. Building on a common model framework, we develop several additional models that can be used to investigate specific aspects of cyber operations on kinetic combat.

14. SUBJECT TERMS cyber, combat model, Lanchester equations, epidemic model			**15. NUMBER OF PAGES** 125
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MODELING THE EFFECTS OF CYBER OPERATIONS ON KINETIC BATTLES

Fatih Yildiz
Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
June 2014

Author: Fatih Yildiz

Approved by: David Alderson
Thesis Advisor

Donald P. Gaver
Co-Advisor

Patricia Jacobs
Second Reader

Robert F. Dell
Chair, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis considers the effects of cyber operations on kinetic warfare, by exploring and building on two recently proposed extensions to traditional Lanchester models of combat. In one model, we consider instantaneous changes to kinetic fighting capability resulting, for example, from the disruption or restoration of communications or other supporting cyber systems. Such changes create discontinuous shocks in the overall combat dynamics and can dramatically affect the outcome of a battle. In the second model, we represent cyber operations as a continuous process of degradation and recovery in fighting capability based on the dynamics of epidemic spread. By using analytical and numerical approaches, we obtain insights about the effect of cyber operations on battle duration and attrition, how cyber operations can affect victory conditions, and tradeoffs in the allocation of limited resources to cyber operations and kinetic operations. Building on a common model framework, we develop several additional models that can be used to investigate specific aspects of cyber operations on kinetic combat.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

"Cyber operations" is topic of increasing importance to the United States and countries all over the world. The impacts of cyber operations on conventional kinetic battles are an area of interest. These operations can be used to decrease fighting capabilities of an adversary. And unlike the study of traditional warfare, there are no well-accepted models for these phenomena. But, the mathematical models for cyber operations can give insights that help strategic decisions to generate tactical approaches. These models can also be used in the efficient allocation of resources.

This thesis is based on Lanchester equations as the main model of combat. Specifically, we build upon two recent efforts that use modified versions of Lanchester equations to study the effect of cyber operations on kinetic battles. In this representation, a cyber attack does not kill an adversary, but it affects fighting capability as represented by the attrition coefficients in the model. The cyber attacker benefits from this action by decreasing the attrition rate of self.

The first model builds on the work of Schramm (2012), in which instantaneous changes to kinetic fighting capability result from, for example, the disruption or restoration of communications or other supporting cyber systems. Such changes create discontinuous shocks in the overall combat dynamics and can dramatically affect the outcome of a battle. We consider a model in which one side suffers a first shock that degrades fighting capability and then another shock that restores it. We explore the impact of timing, duration, and magnitude of the shock on the overall battle outcome.

The second model follows the work of Schramm and Gaver (2013), in which the dynamics of combat are mixed with the dynamics of epidemic spread. Here, cyber operations are represented as a continuous process of degradation and recovery in fighting capability. Again, the analysis focuses on the rate of spread and recovery and its impact on battle outcome.

The main difference between these two models is that, the first one considers a cyber attack at an instant of time, while the second model considers the effect of the

cyber attack as a process evolving over time. Both of these assumptions have different applications and capture different aspects of cyber operations.

In this study, we also propose various extensions to studied models, such as adding different intrusion times, defense capabilities or adding a second type of infection to the system. These proposed models are intended to represent different aspects of cyber operations, and serve as a basis for future work in this area.

LIST OF REFERENCES

Schramm, Harrison C. (2012). "Lanchester models with discontinuities: An application to networked forces." *Mil. Oper. Res. 17*(4), 59–68.

Schramm, H. C., & Gaver, D. P. (2013). Lanchester for cyber: The mixed epidemic combat model. *Naval Research Logistics*, *60*(7), 599–605.

ACKNOWLEDGEMENTS

To my advisors, my professors, my friends, and above all, to my wife.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

"Cyber" is a new term in our lives, a term that is changing business, social relations, politics, and art as well as security-related topics. The use of the prefix "cyber" was first popularized by Norbert Wiener (1965) through his book *Cybernetics, or Control and Communication in the Animal and the Machine*. More recently, this prefix has been associated broadly with the interface between man and machine. The *Merriam-Webster Dictionary* defines cyber as "of, relating to, or involving computers or computer networks (as the Internet)."

A. THE GROWING IMPORTANCE OF CYBER SECURITY

"Cyber operations" is topic of increasing importance to the United States and countries all over the world. Over the last several years, concerns over the effects of cyber security, in particular, were in the spotlight. For example: in 2008, President Bush launched the Comprehensive National Cyber Security Initiative. The North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) was formally established in 2008 in order to enhance NATO's cyber defense capability. In 2009, President Obama directed a "clean slate" Cyberspace Policy Review, which considers "strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (White House, 2009). This review recommended keeping cyber security a top priority for the President. In 2010, the "Cyber domain" was declared as the fifth domain of battleground for the United States (Lynn, *The Economist*, 2010). Recently, President Obama stated cyber security is at the top of the list of priorities for the United States (Obama, 2013).

The main reason for this sharp increase in the importance of cyber-related issues is our increased dependency on electronics. The development of electronic devices and digital networks has been primarily for new functionality, convenience, and cost savings. In most cases security has not been an important issue in the design until there is a cyber-related accident or an intentional breach, known as a cyber security incident. With increased dependency on electronics, security gaps have become even wider.

A second reason for greater attention to cyber-related concerns is the increase in cyber security incidents. In 2011, Symantec reported that over 5.5 billion attacks were blocked, nearly 5,000 new vulnerabilities were identified, and an average breach exposed 1.1 million identities, in computer systems all over the world (Symantec, 2012). Further, over 400 million unique variants of malware attempted to take advantage of those vulnerabilities; with the number of malware variants 40% higher than in 2010. According to a Symantec report in 2014, there were 215 significant incidents of identity theft in 2013 and the average number of exposed identities increased to 1.6 million identities per breach. Moreover, 70% of these identities included real names, 40% included government-issued social security numbers, and 40% included dates of birth. According to the same report, there were 6436 cyber vulnerabilities identified in 2013, eight of which were “zero-day” vulnerabilities, meaning that they were exploited before they were known by cyber security managers (Symantec, 2014).

Another reason for increased attention to cyber security is that cyber operations are fundamentally asymmetric. Only a small amount of resources are needed to create and exploit one’s cyber vulnerabilities. As noted by the Defense Science Board (2013), for as little as $40 up to $4,000 anyone can acquire cyber attack tools. With such a low barrier to entry, almost anyone can exploit any known and uncorrected vulnerabilities.

In the current operating environment, the superiority of U.S. military systems is critically dependent upon increasingly vulnerable information technologies. The Department of Defense (DOD) seeks new techniques, procedures, and technologies to strengthen this link in the chain.

Until recently, there were no mathematical models for cyber operation effects on the battleground. In 2009, the U.S. Department of Homeland Security published the framework, *A Roadmap for Cybersecurity Research*, which identified 11 challenging and vital problems such as identity management, survivability of time critical systems, insider threats, and combating malware. Another well-known study, the JASON Report *The Science of Cyber-Security* (McMorrow, *JASON DTIC Document*, 2010) recommended that all types of analytical approaches should be considered, and it suggested a combination of models from various other sciences such as physics, biology, and epidemiology. In 2011, the *DOD Strategy for Operating in Cyberspace* (DOD, 2011) established a conceptual framework based on five strategic initiatives, summarized as: treat cyberspace as an operational domain, employ new defensive concepts, enhance the government partnership with industry, establish partnerships with allies, invest in research and development.

For a more detailed report on the commercial aspects of cyber operations see Sommer (2011), which discusses a report by Organization for Economic Co-operation and Development (OECD) titled "Reducing Systematic Cybersecurity Risks." For a detailed literature review on military concerns related to cyber operations see the report of the Defense Science Board in 2013 to the Department of Defense titled "Resilient Military Systems and the Advanced Cyber Threat" (Defense Science Board, 2013).

B. SCOPE AND OBJECTIVES OF THIS STUDY

The objective in this thesis is to study the essence and behavior of cyber operation effects on combat. The scope of this study is limited to the description and exploration of the effects of cyber operations within kinetic battle, in order to give descriptive insights of the results of integrated and joint cyber operations.

This study builds on two recent efforts to model the effects of cyber operations in kinetic warfare. Schramm (2012) proposes a mathematical model in *Lanchester Models with Discontinuities: An Application to Networked Forces* to represent shock effects on networked forces, which can be used to represent the results of cyber operations. This study introduces a novel twist on traditional Lanchester equations (Lanchester, 1916)

describing force-on-force combat. Specifically, Schramm considers a discontinuous "shock" that instantaneously changes attrition coefficients in the system of differential equations, and then assesses the impact of this change on the outcome. The shock may be due to a cyber attack which results in decreased effectiveness of the force being cyber attacked. The cyber attack affects the opposing force permanently to the end of the battle. This representation naturally leads to questions about the timing and degradation of fighting capability: how much weaker can a force become and still win? How long must a cyber attack be effective to result in a kinetic battle victory?

Following this, Schramm and Gaver (2013) propose a "mixed epidemic combat model" that models cyber attacks as variants of biological infections, which affect the kinetic fighting capability of the opposing force. The basic scenario is as follows: A *Red* force kinetically attacks a *Blue* force while also trying to infect *Blue*'s electronic devices with a cyber attack in order to reduce *Blue*'s defensive power and offensive power. The *Blue* force attacks *Red* kinetically only, but with reduced capability because of infection. While the battle goes on, *Blue* forces try to cure the cyber infection to return the infected units to full capability. Thus, the cyber attack on *Blue* may change the battle outcome, and even if *Blue* were the dominant power before being affected by an infection, the battle may result in a *Red* victory.

Following the work of Schramm (2012) we assume that a cyber incident can degrade the fighting capability of a force. We extend the model by representing recovery of the degraded force. **Results from this model provide insights about the effect for kinetic battle of the time of the cyber attack and recovery, and supply a tool to compare the metrics of a cyber incident with the kinetic battle.**

Following the lead in Schramm and Gaver (2013), in this thesis we assume that cyber operations can take the form of malware, and cyber attacks can be represented as variants of biological infections. We extend the mixed epidemic combat model to a two-sided setting. **Results from this model provide insights into the tactical use of cyber operations.**

The main objective of the models is to explore issues related to how cyber operations affect battle duration, how cyber operations affect victory conditions, and under which conditions the victorious side can change as a result of the cyber operation. Specific measures of performances include: how cyber operations affect battle duration and attrition; how cyber operations affect victory conditions. Other questions of interest include allocating limited resources for cyber operations and kinetic operations and how to allocate the limited resources to cyber operations and kinetic operations.

C. ORGANIZATION OF THIS THESIS

The remainder of this thesis is organized as follows. Chapter II contains a literature review of studies related to cyber operations, as well as other studies involving kinetic warfare models with three nature-inspired models and cyber operation effects on kinetic warfare models. Chapter III introduces the first model about cyber operations on kinetic battles, treating cyber operation as a discrete pulsed effect. We extend the original model by modifying the model for recovery. In Chapter IV, we introduce the original cyber epidemic combat model, propose an extended two-sided cyber epidemic combat model, and explore the proposed model for different aspects. In Chapter V, we propose new models by extending the assumptions in studied models. These models are generated to explore specific application areas. In Chapter VI, we conclude the thesis by giving the insights derived, which is followed by our operational recommendations, and directing future studies for appropriate research areas to fill the gaps. In the appendices, we describe in detail the steps we used to develop the proposed model and some proposed formulation.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

The use of cyber operations in military conflict is now more than 30 years old. Cyber space is well-integrated with conventional kinetic combat domains. Cyber operations, unlike conventional warfare, can be applied on a broader scale. All communication systems, radars, missile launchers, and high tech weapons as well as infrastructure networks, financial institutions, electronic media, and power grids belong to the cyber domain. All of these systems are potential targets of cyber operations (Cigital, 2013). To illustrate the range of the cyber threat, we highlight some past cyber events in the following section.

A. HISTORY OF CYBER OPERATIONS

In 1998, the first step for a cyberwar in a real kinetic battle was recorded. An information operations cell was established by NATO to electronically attack critical network infrastructure and command and control systems in the Kosovo war. Because of this, the air campaign operation against targets in Serbia was especially successful throughout the 78 days of operation according to a special report for the U.S. Air Force (Grant, 1999). During Operation Allied Force, Serbian forces hacked into NATO Internet pages, erased email archives, and made email pages unavailable for some time (Hancock, 1999).

In 2000, in an operation named Moonlight Maze by American Intelligence, U.S. officials discovered a pattern of probing of computer systems at the Pentagon, NASA, the U.S. Department of Energy, private universities, and research labs. This attack began in March 1998 and continued for nearly two years. During this time, vast amounts of data consisting of research and development secrets were stolen and sent over the Internet to Moscow to sell to the highest bidder. Moreover, according to the testimony of James Adams, CEO of Infrastructure Defense, Inc., the commercial value of stolen information varied from tens of millions of dollars to hundreds of millions of dollars (Adams, 2013).

Disturbingly, some of the most sensitive and secure federally-owned networks have been compromised. In 2006, the U.S. Naval War College computer network was completely inactive for some time because of the cyber intrusions (Decker and Douglass, 2011). In 2007, the Oak Ridge National Laboratory, where the first atomic bomb was produced, was attacked by a highly educated group who are allegedly Chinese (Decker and Douglass, 2011), in series of cyber attack attempts to a larger penetration of U.S. national security. The same year, a document was leaked about an internal review that reported a Chinese military cyber attack on Pentagon computer networks, including the one used by Defense Secretary Robert Gates (Decker and Douglass, 2011). Also, the U.S. government suffered "an espionage Pearl Harbor" in the same year, in which an unknown foreign power broke into some of the high-tech networks of the military agencies, and stole terabytes of information (Shamah, 2013).

Moreover, cyber attacks have targeted U.S. military computer systems installed overseas. In 2008, a hacking incident occurred on a U.S. military facility in the Middle East. United States Deputy Secretary of Defense William J. Lynn III had the Pentagon release a document, which noted that "malicious code" on a USB flash drive spread undetected on both classified and unclassified Pentagon systems, establishing a digital beachhead from which data could be transferred to servers under foreign control. "This was the most significant breach of U.S. military computers ever and it served as an important wake-up call," Lynn wrote in an article for *Foreign Affairs* (Lynn, 2010).

In 2010, for the first time the United States publicly warned of the Chinese military's use of civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies. DOD also pointed to an alleged China-based computer spying network dubbed GhostNet that was revealed in a research report in 2009. The DOD stated: "The People's Liberation Army is using "information warfare units" to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals" (DOD, 2009).

The U.S., of course, is not the only target of cyber attacks. In 2010, a specially designed computer virus, Stuxnet, was revealed. It was a revolution in special cyber weapons. It was designed to spread on microchips, which means any electronic device that

is not a computer. It spread on electronic systems mostly in Iran to decrease the uncontrolled nuclear development, and it destroyed ~1000 uranium centrifuges out of 5000, causing a capacity decrease of 20% (Sanger, 2012).

More recently, attacks have become more damaging and more focused on specific weapons development programs. In 2012, according to a report prepared for the DOD by the Defense Science Board, Chinese hackers have gained access to designs of more than two dozen major U.S. weapons systems. *The Washington Post* said that these designs included combat aircraft and ships, missile defense systems including the Patriot missile system, the Navy's Aegis ballistic missile defense systems, the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the F-35 Joint Strike Fighter (Nakashima, 2013).

Equally dangerous are attacks targeting the national economy. In 2012, distributed denial of service (DDoS) attacks were carried out against the New York Stock Exchange and a number of banks, including J.P. Morgan Chase. Credit for these attacks was claimed by a hacktivist group called the Qassam Cyber Fighters, which have labeled the attacks "Operation Ababil." The attacks had been executed in several phases and were restarted in March 2013. The size of the attacks (65 gigabits/second) is more consistent with a state actor than with a typical hactivist DoS attack (~2 gigabits/ second) (Gonsalves, 2012). Such threats are not reserved for the U.S. alone. In 2013 an attack was launched against South Korea. A logic bomb struck machines "and wiped the hard drives and master boot records of at least three banks and two media companies simultaneously" (Singel, 2010).

Overall, the amount of malicious code generated over the world is increasing exponentially (see Figure 1), which affects the military networks as well as infrastructure, government and supply chain related networks. Moreover, with an increased dependency on cyberspace, the complexity of the tools and the harmful effects of these infected codes can become increasingly dangerous.

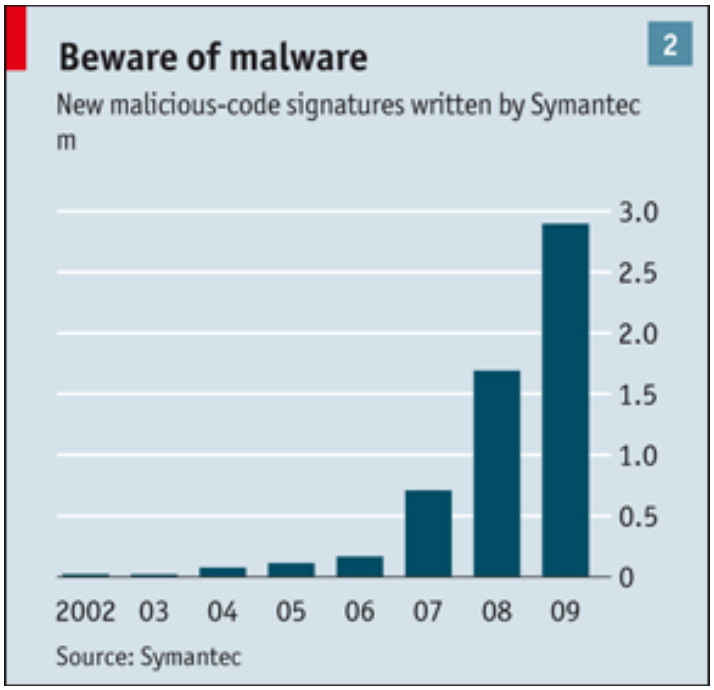

Figure 1. New types of malicious codes increased dramatically in the recent years. The units are in millions (from *The Economist*, 2010).

B. BUILDING BLOCKS

Lanchester models are well-understood ordinary differential equation (ODE) models to explain mutual attrition behaviors in combat.

Cyber warfare is not a well-understood phenomenon, and does not have a single well-studied and commonly accepted mathematical model. We study two different models which capture different aspects of cyber warfare. We aim to explore the effect of recovery by using closed form Lanchester models, and we aim to capture the essence of "exploiting vulnerabilities by spreading malicious code" behavior of cyber operations by using ODE models of disease spread.

This section reviews the basic structure and terminology for each model.

The combat models of Schramm (2012) include *shock effects*, which change some attributes of fighting forces. We use the shock effects to represent *cyber effect*s (*cyber attack*) on a force, which change the fighting capabilities of the force. Fighting capabilities include *kinetic capabilities (kinetic attack)* which are represented by Lanchester aimed-

fire. *Attrition* is a result of kinetic attack only, and cyber effects do not cause attrition. We use two shock effects in the battle one representing the cyber attack, and the other representing the *recovery* of the effects of the cyber attack. We refer to *shock time* as the time the cyber attack (first shock) happens, and *recovery time* as the time the force recovers (second shock) back to original attributes. We use two opposing forces in the model, named *Red force (Z)* as cyber attacker, and *Blue force (B)* as cyber defender, unless stated otherwise.

Schramm and Gaver (2013) combines *kinetic battle models (Lanchester models)* with an epidemiological model of disease progression for cyber operations. These models represent numbers of fighting forces, which change due to a physical loss of a part of the force (*attrition*). Lanchester models use *attack rate (kinetic attack rate)* to represent the number of effective shots (or kills) on the adversary. The attack rate represents not only the rate of fire by the attacker, but also represents the rate of successful defense (shielding) by the defender. So, the attack rate of *Blue* (to *Red*), is equivalent to the *attrition rate* of *Red*. Attrition can be a result of *kinetic combat* (*kinetic battle, conventional combat*) only, and infection can be a result of *cyber operation (cyber attack)* only. A force which can conduct an offensive cyber operation has a *cyber attack capability*. A force which has assets and procedures (*defensive cyber actions*) to reduce the effect of a cyber attack, has a *cyber defensive capability*. A cyber attack may cause a loss of capability (*cyber infection, infection*) on the adversary, and cyber defense may reduce this degrading effect. We assume in this study that these two capabilities go side by side, and any force with cyber attack capability also has cyber defense capability. However, one cyber capability may be stronger than the other.

The term *infection (disease)* used in this study is a broad term, which can be used for any effect that reduces a force's warfighting capabilities, and is not lethal. In this study, this effect is limited to cyber malware. It can be defined differently, in order to model different effects. We use *infected unit* to describe any unit affected by a cyber attack. This type of infection is designed to *spread* in the cyberspace, using system gaps and backdoors, which we call *vulnerabilities*. A detailed definitions list for technical terms is added in Appendix A.

1. Combat (Kinetic) Models

Lanchester Models are the main combat models used in this study. We limit the models to Aimed-fire and Area-fire, but the models can be used in various ways. These models use differential equations to describe changes in the surviving force levels in a combat. Each force is assumed to consist of homogeneous units in terms of their geography and range. For each force, we assume that we can calculate an overall kill rate per instant of time (*dt*). For the Aimed-fire model, we assume that these shots are aimed at individual adversarial live targets. For the Area-fire model, we assume that an area of interest is under fire (e.g., artillery, mortar, air support), without considering specific target attributes. Although these two models seem similar, their units of measures are different, and we cannot compare the results from these two models directly.

We summarize these two models as follows.

a. Aimed Fire

For *Aimed-fire*, the basic equations area::

$$\frac{dB(t)}{dt} = -\rho\, Z(t), \qquad (2.1)$$

$$\frac{dZ(t)}{dt} = -\beta\, B(t). \qquad (2.2)$$

Here, *B(t)* is the number of overall alive Blue units at time *t*, and *Z(t)* is the corresponding number of overall alive Red units. The term $\frac{dB(t)}{dt}$ means the change in the Blue force in *dt*, and ρ represents the constant attack rate of Red. So, in an aimed-fire model, the number of killed in Blue force depends on number of shooters on Red force, and their shooting effectiveness against individual Blue targets. Similarly, $\frac{dZ(t)}{dt}$ represents the change in Red force in *dt*, and β is the constant attack rate of Blue. Note that the recipient of aimed fire is explicitly an active (fighting) member of the opposing force.

Attack rates in these models represent both offensive and defensive measures. That is, there is no explicit means to change the kinetic defense. Defensive measures may be considered when estimating attack rate. The attack rates in these models are all constants. They do not depend on time or size of the force.

The exchange ratio ($\frac{dB(t)}{dZ(t)}$) is the ratio of change in force level of *B(t)* with respect to *Z(t)* in *dt*; it depends on force levels, and attack rate ratios in Aimed-fire models.

b. Area Fire

For *Area-fire*, the basic equations are:

$$\frac{dB(t)}{dt} = -\rho\, Z(t)\, B(t), \qquad (2.3)$$

$$\frac{dZ(t)}{dt} = -\beta\, B(t)\, Z(t). \qquad (2.4)$$

Here, the number of Blue units killed in the Area-fire model depends on number of Red shooters, number of targets on the area (density), and Red's shooting effectiveness. The exchange ratio ($\frac{dB(t)}{dZ(t)}$) does not depend on force levels, and solely depends on attack rates in the Area-fire model.

Aimed-fire and *Area-fire* models are the most commonly used combat models. They are crude, but roughly explanatory. Using experimental data and proper tools, combat factors can be understood and even can be predicted. Figure 2 compares a Lanchester aimed-fire model with reinforcements to real data from the well-known study of the 1945 Battle of Iwo-Jima (Engel, 1954).

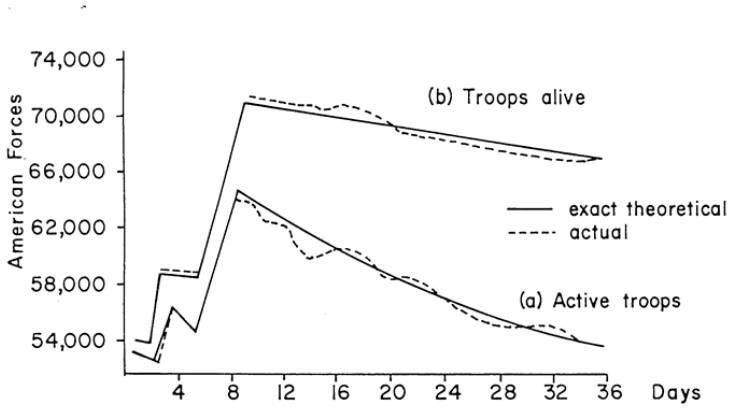

Figure 2. Comparison of the Lanchester model outcome and real results for the 1945 Battle of Iwo-Jima (from Engel, 1954).

2. Epidemic Models

The commonly used mathematical models in epidemiology are *S-I* and *S-I-R* models. An overall population is partitioned into three groups, described as susceptible (S), infected (I), and recovered (R) (Murray, 2002). Although there are more detailed and expanded infection models, we use the S-I-R model as a base model, as was used in Schramm and Gaver (2013), and use it to construct later models.

Epidemic models are classified by the spread type. We use Kermack-McKendrick type spread in this study, which is consistent with general S-I-R models, but we will not consider natural births, deaths, migration, or partial immunization as studied in the paper (Kermack and McKendrick, 1927). Although there are different types of infection spread models (i.e., Lanchester infection, Daley-Kendall infection, Michaelis - Menten infection etc.), for different environments and assumptions, we will use a simple, generalized, and well-studied model for infection spread.

For a fixed population of size N, $N = S(t) + I(t) + R(t)$, where *S(t)* (respectively *I(t)* and *R(t)*) is the number of population members that are susceptible (respectively infected and recovered) at time *t*. The original Kermack and McKendrick (1927) epidemic model is:

$$\frac{dS(t)}{dt} = -\Psi\ S(t)\ I(t), \tag{2.5}$$

$$\frac{dI(t)}{dt} = \Psi\ S(t)\ I(t) - \gamma\ I(t), \tag{2.6}$$

$$\frac{dR(t)}{dt} = \gamma\ I(t). \tag{2.7}$$

The term $\frac{dS(t)}{dt}$ represents the change in the subpopulation susceptible to the disease, which depends on the contacts between members that are infected and susceptible, and spread rate *(Ψ)*. The term $\frac{dR(t)}{dt}$ represents the change in the subpopulation recovered from the disease, in this case equal to the cure rate *(γ)* times the number infected. The term $\frac{dI(t)}{dt}$ represents the change in number of the population that is infected, by using other two equations because the population total *(N)* is constant.

We use these models to explore different aspects of cyber warfare on kinetic battles. Appendix C discusses the methodology we use to understand and explain these models.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DISCRETE CYBER EFFECTS

In this chapter, we consider the discrete effects of cyber operations on combat. We build on the work of Schramm (2012), who considers a kinetic battle between two opponents, one of whom suffers a discontinuous "shock" that instantly degrades its fighting capability. An important aspect regarding this model is that only the kinetic battle results in attrition. The cyber effect does not cause any attrition, but changes its pace. The motivating idea is to consider a fighting force whose effectiveness derives from its ability to coordinate its operations using a communications and/or computer network. The degradation to fighting capability comes from the loss of the network, which is presumed to happen suddenly (e.g., from a cyber attack by the opponent). Schramm explores the impact of the timing and size of this shock on the kinetic battle.

We extend this work by adding a second shock that cures the impacts of the first shock (e.g., corresponding to a restoration of the underlying network). This second shock helps to limit the effects of the cyber attack, and helps to quantify its impact on overall attrition. We restrict attention to Lanchester aimed fire calculations in this chapter.

We begin with a summary of Schramm (2012). Consider a battle involving aimed fire. Consider the case where Blue suffers a shock at time t_* that decreases Blue's attack rate from β_U to β_D, where $\beta_D < \beta_U$. The modified Lanchester equations then become the following.

$$\frac{dZ(t)}{dt} = -\beta_U B(t), \qquad t < t_* \tag{3.1}$$

$$\frac{dZ(t)}{dt} = -\beta_D B(t), \qquad t_* \leq t \tag{3.2}$$

$$\frac{dB(t)}{dt} = -\rho_U Z(t), \qquad \forall\, t \tag{3.3}$$

A. EXPLORATION OF LANCHESTER MODELS WITH DISCONTINUITIES

In their most general form, let $\beta(t)$ denote the instantaneous attack rate of Blue (on Red) at time *t*, and similarly let $\rho(t)$ denote the attack rate of Red (on Blue). The general form of the Lanchester equations is as follows:

$$\frac{dZ(t)}{dt} = -\beta(t)B(t), \tag{3.4}$$

$$\frac{dB(t)}{dt} = -\rho(t)\,Z(t), \tag{3.5}$$

$$\frac{dZ(t)}{dB(t)} = \frac{\beta(t)}{\rho(t)}\frac{B(t)}{Z(t)}, \tag{3.6}$$

$$Z(t)\;dZ(t) = \frac{\beta(t)}{\rho(t)}\,B(t)\;dB(t), \tag{3.7}$$

$$\int_0^t \rho(t)\,Z(t)\,dZ(t) = \int_0^t \beta(t)\,B(t)\,dB(t). \tag{3.8}$$

The case where Blue suffers a single shock degrading its combat capability corresponds to the following attack rates:

$$\rho(t) = \quad \rho,\ 0 \le t < t_f$$

$$\beta(t) = \begin{cases} \beta_U,\ 0 \le t < t_* \\ \beta_D,\ t_* \le t \le t_f \end{cases}$$

Let t_f denote the time at which the battle ends. We define the following mathematical terms:

B(t = 0) = B_0 , Z(t = 0) = Z_0 → Initial number of force units,

B(t = t_*) = B_* , Z(t = t_*) = Z_* → Number of force units at the time of shock,

B(t = t_f) = B_f , Z(t = t_f) = Z_f → Number of force units at the end of the battle.

Throughout this analysis we assume that $B_0 > B_* > B_f$ and $Z_0 > Z_* > Z_f$. To evaluate for B_* and Z_* , we use the numbers just before the time of shock, to be consistent.

We can rewrite the equation for given model Eq. (3.8):

$$\rho \int_{t_f}^{0} Z \, dZ = \beta_U \int_{t_*}^{0} B \, dB + \beta_D \int_{t_f}^{t_*} B \, dB . \qquad (3.9)$$

This implies that:

$$\rho \left(Z_0^2 - Z_f^2\right) = \beta_U \left(B_0^2 - B_*^2\right) + \beta_D \left(B_*^2 - B_f^2\right). \qquad (3.10)$$

The end of the battle can be set when the force size of one side (Red) is 70% of initial number of units, or the force size of the other side (Blue) is 50% of initial number of units. For simplicity, we use fight to the finish in this study. In case of a fight to the finish, at the end of the battle one of the force sizes would reach zero.

The new dynamic state equation (with shock) is:

$$B_*^2 - B_f^2 = \frac{\beta_U \left(B_0^2 - B_f^2\right) - \rho \left(Z_0^2 - Z_f^2\right)}{\beta_U - \beta_D}. \qquad (3.11)$$

We can summarize the dynamic state equations both without and with cyber effect:

$\beta_U \left(B_0^2 - B_f^2\right) - \rho \left(Z_0^2 - Z_f^2\right) = 0$ → *Without cyber effect*

$\beta_U \left(B_0^2 - B_f^2\right) - \rho \left(Z_0^2 - Z_f^2\right) = \left(B_*^2 - B_f^2\right)(\beta_U - \beta_D)$ → *With cyber effect.*

The difference in the dynamic state equation caused by the cyber attack of Red on Blue is:

$$\left(B_*^2 - B_f^2\right)(\beta_U - \beta_D). \qquad (3.12)$$

Note that regardless of the victorious side, one of B_f or Z_f will be zero and the other one will be positive, which represents the survivors from the battle when the battle is over and there is no more cyber attack. We refer to this case as "no recovery," because in this case Blue was attacked but did not recover, and continued to fight with degraded attack rate β_D.

We display the results of a numerical experiment in Figure 3 and Figure 4. Both sides start with same initial numbers, but with different attack rates. We increased the detail level in the graphs by using 10 steps in 1 time (*t*), **and to reproduce these figures, time should be divided by 10.**

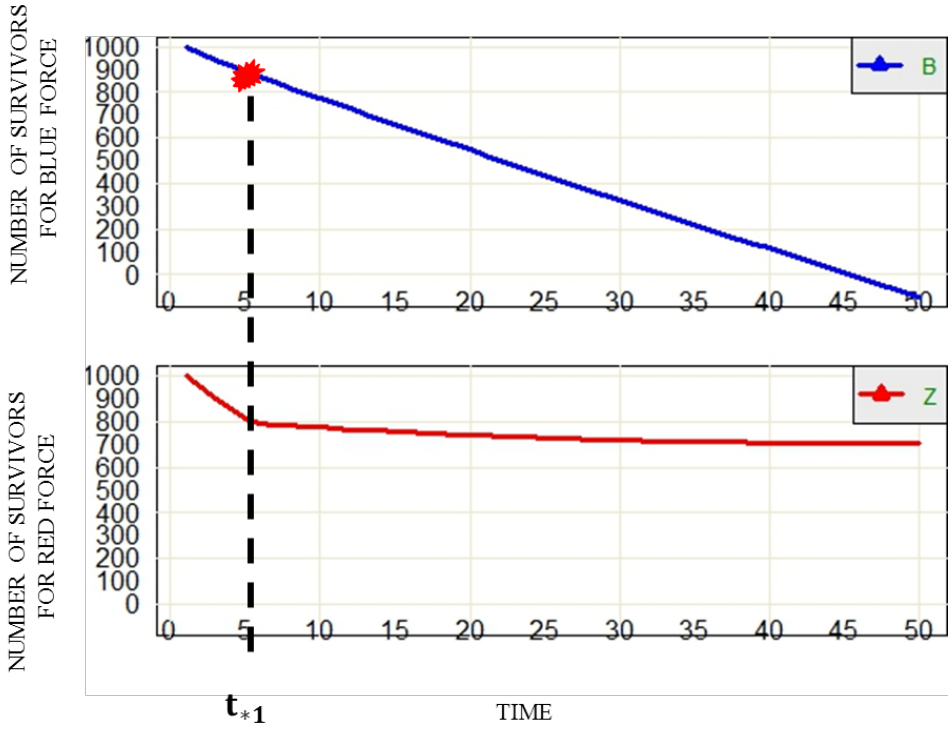

Figure 3. One-sided shock effect on number of survivors.
Given initial force sizes $B_0 = Z_0 = 1000$, the battle begins with $\beta_U = 0.5, \rho = 0.3$
However, at time t_{*1} , Blue suffers a shock that reduces its attack rate to $\beta_D = 0.05$
Despite the initial fighting superiority of Blue, Red wins the battle.

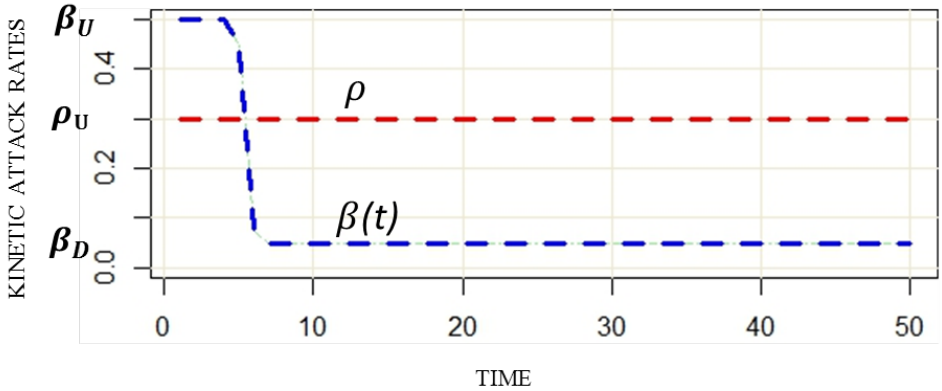

Figure 4. Shock effect on Blue's kinetic attack rates.
(Time is multiplied by 10 on both figures)

Figure 3 shows the change in number of units for both sides throughout the combat. At t_{*1} we see a change in Blue's attack rate, which (we assume) is caused by a cyber attack launched by Red (Figure 5).The cyber attack affects the attrition of both sides. Explicitly, it enables Red to win despite an initial fighting inferiority.

B. DISCONTINUOUS DEGRADATION AND RECOVERY

We next consider the case where Blue suffers but then recovers from a cyber attack. We do this through the use of two shocks, in which the first one downgrades the attack rate of the Blue to β_D and the second one upgrades the attack rate back to normal β_U. Let t_{*1} denote the time of the first (degrading) shock, and let t_{*2} denote the time of the second (recovery) shock. The corresponding attack rates for each side are:

$$\rho(t) = \quad \rho, \quad 0 \le t \le t_f$$

$$\beta(t) = \begin{cases} \beta_U, & 0 \le t < t_{*1} \\ \beta_D, & t_{*1} \le t < t_{*2} \\ \beta_U, & t_{*2} \le t \le t_f \end{cases}$$

Dropping the explicit time dependence for *B* and *Z*, we write the battle equations as:

$$\frac{dZ}{dt} = -\beta_U B, \qquad 0 \le t \le t_{*1} \tag{3.13}$$

$$\frac{dZ}{dt} = -\beta_D B, \qquad t_{*1} \le t < t_{*2} \tag{3.14}$$

$$\frac{dZ}{dt} = -\beta_U B, \qquad t_{*2} \le t \le t_f \tag{3.15}$$

$$\frac{dB}{dt} = -\rho_U Z, \qquad \forall\, t\ . \tag{3.16}$$

Now we use the same numerical experiment as Figure 3 and Figure 4, but we implement the second shock to the system. Now Blue is degraded by a cyber attack at t_{*1} and Blue recovers from the cyber attack at t_{*2}. Both sides start with same initial numbers, but with different attack rates. Figure 5 and Figure 6 can be compared to Figure 3 and Figure 4 to visually see the effects of recovery at t_{*2}.

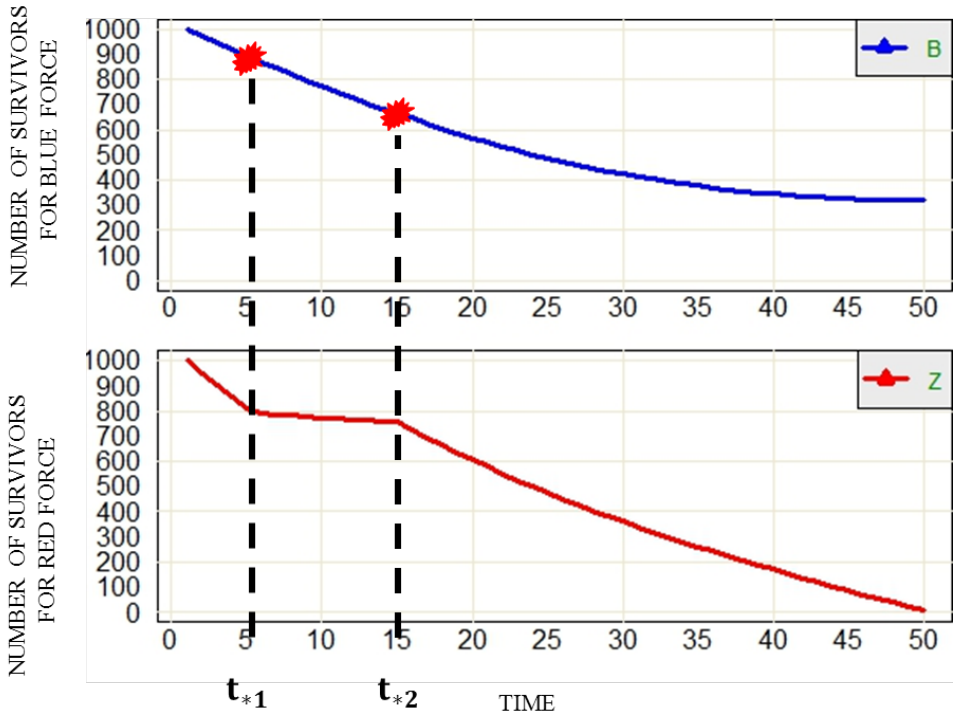

Figure 5. Effect of two shocks on number of survivors.

Here, Blue suffers a degradation at time t_{*1} but recovers at t_{*2} and is still able to win the battle (Time is multiplied by 10.).

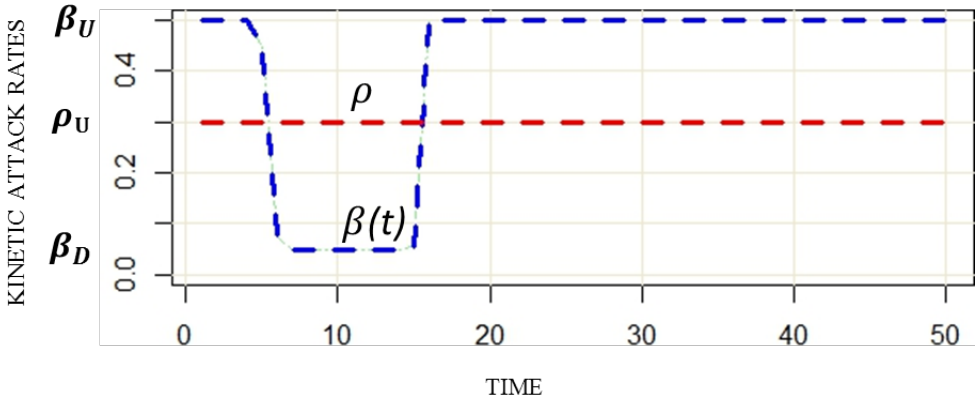

Figure 6. Two shock effects on kinetic attack rates.
(Time is multiplied by 10.)

Figure 5 shows the change in number of units throughout the combat, in case of two shocks. Figure 6 shows the change in kinetic attack rates of forces. At t_{*1} we see a drop in Blue's attack rate, and at t_{*2} it recovers. These figures show how the recovery from a cyber attack affects the attrition of both sides. Explicitly, it changes the pattern of Red, and the change in Red causes a change in Blue. Now Blue wins the battle, again.

Using the same notation, and keeping the same set of assumptions as $B_0 > B_{*1} > B_{*2} > B_f$ and $Z_0 > Z_{*1} > Z_{*2} > Z_f$, which means that the cyber attack happens (t_{*1}) before recovery (t_{*2}). Note that t_f cannot be smaller than t_{*2}, and t_{*2} cannot be smaller than t_{*1} for a logical sequence. They can be equal, but then there would be no change in state equation. We can rewrite the equation (3.9) for given model:

$$\rho \int_{t_f}^{0} Z\, dZ = \beta_U \int_{t_{*1}}^{0} B\, dB + \beta_D \int_{t_{*2}}^{t_{*1}} B\, dB + \beta_U \int_{t_f}^{t_{*2}} B\, dB\,. \qquad (3.17)$$

The closed form of the equations is, *in this special case*:

$$\rho\left(Z_0^2 - Z_f^2\right) = \beta_U\left(B_0^2 - B_{*1}^2\right) + \beta_D\left(B_{*1}^2 - B_{*2}^2\right) + \beta_U\left(B_{*2}^2 - B_f^2\right). \qquad (3.18)$$

The expression B_{*1}^2 uses the number of Blues at the time of the successful cyber attack, and the expression B_{*2}^2 uses the number of Blues at time of full recovery from cyber-affected targets. The term $(\beta_U - \beta_D)$ represents the reduction in kinetic attack rate due to a successful cyber attack.

The dynamic state equation in this case is:

$$B_{*1}^2 - B_{*2}^2 = \frac{\beta_U\left(B_0^2 - B_f^2\right) - \rho_U\left(Z_0^2 - Z_f^2\right)}{\beta_U - \beta_D}, \qquad (3.19)$$

We can summarize the dynamic state equations as:

$\beta_U\left(B_0^2 - B_f^2\right) - \rho\left(Z_0^2 - Z_f^2\right) = 0$ → *Without cyber effect*

$\beta_U\left(B_0^2 - B_f^2\right) - \rho\left(Z_0^2 - Z_f^2\right) = \left(B_{*1}^2 - B_{*2}^2\right)(\beta_U - \beta_D)$ → *With cyber effect.*

In this case change in the dynamic state equation by the cyber attack of Red to Blue is:

$$(\mathrm{B}_{*1}^{2} - \mathrm{B}_{*2}^{2})\ (\beta_{\mathrm{U}} - \beta_{\mathrm{D}}). \tag{3.20}$$

which is the same result with one shock. The reason for the square is because we use an underlying square law (aimed fire) in the model. This would be a straight multiplication if we used a linear law (area fire).

We can also adapt (3.19) for the cases with **strictly one** shock (no cure), if we use the second shock time as the end of the battle ($t_{*2} \leq t_f$). We should point out that the end of battle can be predefined as a level (i.e., percentage, number) for any of two sides; however we use a fight to the finish assumption to obtain a clear picture of the model results.

(3.12) is another important equation which provides us an intuitive result concerning how a cyber attack on one side (B here) can change the opponent's effectiveness, and can change the overall battle result. The cyber attack to Blue causes a difference in dynamic state equation as much as $(B_{*1}^{2} - B_{*2}^{2})\ (\beta_U - \beta_D)$, which shows itself as the reduction in attrition of Red. So if a cyber attack starts at t_{*1} and ends (or cures) by t_{*2}, and the effectiveness drops down to β_D in between these times; assuming that by a cyber attack the whole Blue force is affected, the damage caused by this attack can be summarized as:

$$\boldsymbol{\left(B_{*1}^{2} - B_{*2}^{2}\right)\left(\beta_U - \beta_D\right)}. \tag{3.21}$$

Eqs. (3.19) and (3.21) show that **the period of time between cyber attack time and recovery time is crucial**. Also, if we have a central or a bottleneck cyber target (i.e., a main network server, a communication server), **the size of affected Blue force is crucial**. Both of these terms will greatly boost the effectiveness of Red's cyber attack on Blue, but the reduction in the kinetic attack rate of Blue caused by Red's cyber attack will boost the effectiveness of the cyber attack proportionally.

Similar to previous numerical experiments, we use the same numerical experiment with Figure 5 and Figure 6 but we change the time of second shock. Now Blue is degraded

by a cyber attack at t_{*1} and Blue recovers from the cyber attack at t_{*2}, but the duration in between these two shocks are increased by 30%. Both sides start with same initial numbers, with different attack rates. Figure 7 and Figure 8 can be compared to Figure 5 and Figure 6 to visually see the impacts of timing of recovery (t_{*2}) and the duration (t_{*2}-t_{*1}) of cyber attack effects.

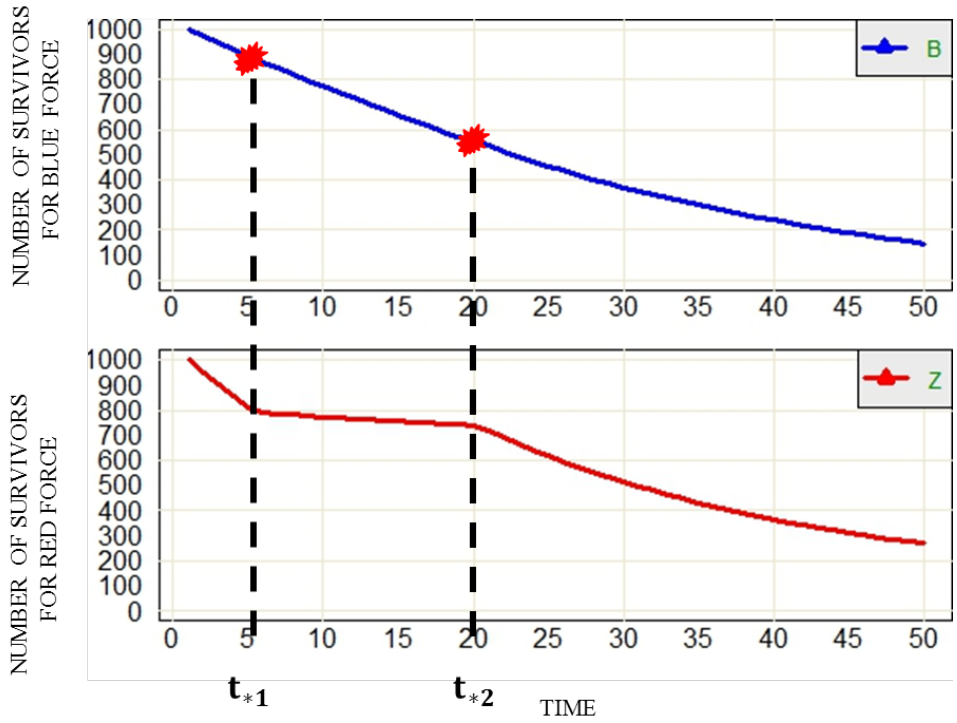

Figure 7. Effect of a longer cyber attack duration on number of survivors. In this case, Blue is degraded long enough for Red to get the advantage and win.

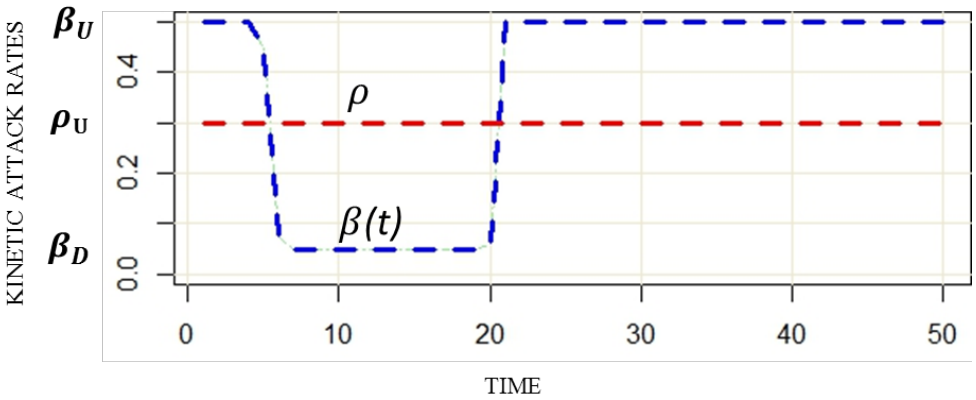

Figure 8. Effect of two shocks on kinetic attack rates for a longer cyber effect time. (Time is multiplied by 10 on both figures)

The increase in time between the two shocks affects the battle significantly and helps the cyber attacker (Red) to win the battle. Figure 7 displays the change in number of units, in case of two shocks for a larger timeframe compared to Figure 5. Figure 8 displays the change in kinetic attack rates of the forces. At t_{*1} again, we see a drop in Blue's attack rate, and at t_{*2} it recovers. Comparing these figures we see that when it takes a longer time (30%) for Blue to recover, Red wins the battle.

C. ADDITIONAL EXTENSIONS

1. Special Case: Recovery Decisions by Blue

Now consider the case in which Blue can make a decision to fight against the cyber attack or not. Since any defensive actions will need some resources, we can compare how many resources Blue should allocate for recovering after a successful cyber attack. When should Blue continue with the kinetic attack (ignore the cyber incident), and when should Blue try to recover?

We showed that without recovering the cyber-affected units, the reduction in the state equation will be until the end of the battle so the difference in the state equation is $\left(B_{*1}^2 - B_f^2\right)(\beta_U - \beta_D)$. Also recovering the cyber affected Blue units, the difference in the state equation can be estimated as $(B_{*1}^2 - B_{*2}^2)(\beta_U - \beta_D)$. That means recovery causes a change in state equation as $\left(B_{*2}^2 - B_f^2\right)(\beta_U - \beta_D)$. Now the question is "is this difference worth allocating resources to recover?"

We can rephrase this expression as, the power of attack gained back (attrition of Red) by Blue recovering from a cyber attack is:

$$\left(\boldsymbol{B_{*2}^2 - B_f^2}\right)\left(\boldsymbol{\beta_U - \beta_D}\right). \qquad \textit{(3.22)}$$

2. Special Case: Reinforcements for Blue

Suppose Blue can obtain one of two types of assistance at time t_{*2}. One is cyber assistance which will increase Blue attack rate back to β_U from β_D. The other type of

assistance will add B_r units to the kinetic battle and Blue's attack rate will remain at the lower rate β_D. Considering that Blue receives a reinforcement unit in number B_r at time t_{*2}, the second shock at t_{*2} can be used for either recovery, or not.

Obviously, if the gain from kinetic battle is greater than the gain from recovery, then the assistance should be used in kinetic combat.

We need to compare two cases for t_{*2}, the case where there is no recovery and use the reinforcements, B_r, with degraded rate, and the case where the assistance is used to recover from the cyber attack. So if, $B_r^2\beta_D > \left(B_{*2}^2 - B_f^2\right)\left(\beta_U - \beta_D\right)$ then Blue should use these assistance (B_r) for kinetic combat; otherwise, use the cyber assistance. Rewriting the equation:

$$\frac{B_r^2}{B_{*2}^2 - B_f^2} > \frac{\beta_U}{\beta_D} - 1\,. \qquad (3.23)$$

Or in other words, assuming this is a fight to the finish battle (e.g., $B_f = 0$), use in the assistance to recover from cyber attack if,

$$\frac{\beta_U - \beta_D}{\beta_D} > \left(\frac{B_r}{B_{*2}}\right)^2. \qquad (3.24)$$

So, this comparison gives some insight about what is most important. If a unit is under cyber attack with a shock such as a computer virus attack, a triggered zero day attack, a DoS (denial of service) attack, a highly centralized target (network bottleneck) attack, etc., we can use this comparison. It means using the kinetic combat assistance if the degraded attack rate does not make much difference or if the additional kinetic force is significantly larger compared to Blue forces in the theater at (estimated) time of recovery.

Numerically, if the arriving force (B_r) is roughly 10% of the size of the recovery time force (B_{*2}), it makes sense to use it in kinetic battle if the decrease in attack rate

because of cyber attack $\beta_U - \beta_D$ is less than 1% of β_D (i.e., cyber attack is very ineffective). However, Blue should use the cyber assistance to recover the affected unit(s) if the decrease ratio to downgrade attack ratio is more than 1%.

Now we have a value for the cyber attack effect to compare and evaluate with kinetic battle $(B_{*1}^2 - B_f^2)(\beta_U - \beta_D)$, and another value for recovering from a cyber attack $(B_{*2}^2 - B_f^2)(\beta_U - \beta_D)$. With the fact that $B_{*1}^2 > B_{*2}^2$, we have a solid background to compare these effects. Under given assumptions, we can generalize that:

If Blue is able to prevent a successful cyber attack at t_{*1}, the gain (prevented loss) will be:

$$(B_{*1}^2 - B_f^2)(\beta_U - \beta_D), \qquad (3.25)$$

If Blue is able to recover from a successful cyber attack, at t_{*2} the gain (prevented loss) will be:

$$(B_{*2}^2 - B_f^2)(\beta_U - \beta_D), \qquad (3.26)$$

These calculations assume that $B_{*1} > B_{*2} > B_f$ for all times t

IV. CONTINUOUS CYBER EFFECTS

In this chapter, we model continuous or gradual effects of cyber operations on combats. We build on the work of Schramm and Gaver (2013), which represents continuous effect by a cyber epidemic model that causes degradation in kinetic capabilities of the cyber infected side. We expand this model by adding cyber capabilities to the infected side, which adds the capability to infect and degrade the kinetic capabilities of the adversary side, also. We explore the interactions of these two cyber epidemics on kinetic battle results, both numerically and analytically.

The spread of a cyber infection is a critical aspect of cyber operation in this model. We assume that a *cyber effect* starts with an infected unit. We control the effectiveness of a cyber attack by changing *infection spread (spread rate, spread)* .The infection decreases the effectiveness of a kinetic attack by degrading the *attack rate*. We use *patch (patch rate)* to describe the cure of infection.

In order to model infection and spread of disease within the fighting population, we assign each fighting unit to one of three states. A unit is in *State S* if it is not affected by cyber infection, but is vulnerable and can be infected at any time. A unit is in *State I (infected)* if it is affected by cyber infection, and such units have a decreased kinetic attack rate within the adversary. A unit is in *State R* if it is immune to the particular infection, either by removing the infection or by using a patch (immunization) for the infection. With time, the number of units in state *S* decreases because susceptible units will be either infected and transformed to state *I*, or cured and transformed to state *R*. Cure before infection is by patching the susceptible, which is *cyber-vaccination* for the infection. The number of units in state *R* increases, because a recovered unit in state *R* will cure its contacts whether they are in state *S* or state *I*. The number of units in a state *I* can either increase or decrease over time, depending on factors, which we shall explore. Modeling infection adds a second layer to combat modeling, so at any time these states will decrease on top of mentioned changes at a constant rate caused by kinetic attacks.

A. THE MIXED EPIDEMIC COMBAT MODEL

We begin with the mixed epidemic combat model of Schramm and Gaver (2013). Capital letters represent state variables which change in time. For ease of understanding, we drop the time-dependence in our notation. So, for instance, *S* represents *S(t).* The original model consists of four differential equations:

$$\frac{dZ}{dt} = -\beta_U(S+R) - \beta_D\,(I)\,, \tag{4.1}$$

$$\frac{dS}{dt} = (-\xi\,S\,I - \eta\,S\,R) - \rho\,Z\,\frac{S}{S+I+R}\,, \tag{4.2}$$

$$\frac{dI}{dt} = (\xi\,I\,S - \eta\,I\,R) - \rho\,Z\,\frac{I}{S+I+R}\,, \tag{4.3}$$

$$\frac{dR}{dt} = (\eta\,S\,R + \eta\,R\,I) - \rho\,Z\,\frac{R}{S+I+R}\,. \tag{4.4}$$

I represents number of infected units in Blue force at time *t*, *S* represents number of susceptible units in Blue force at time *t*, and *R* represents number of recovered (patched) in Blue force at time *t*. The total size of the fighting Blue force is the sum of these variables, i.e., *B=S+I+R,* which decreases in time. Also, *Z* represents total number of fighting Red units, which decreases. These variables change continuously in time. Also, Greek letters represent rates, which are constant coefficients: β_U represents attack rate for each Blue unit that is either susceptible or recovered. β_D represents decreased attack rate of each Blue unit that is infected, and ρ represents normal attack rate of each member of the Red force. There are of attack rates for Blue, because the attack rate is assumed to change after a cyber incident. Also, ξ represents spread rate of the infection in Blue, and η represents cure rate of the infection of Blue, which occurs when a recovered Blue encounters an infected Blue. Also, susceptible members of Blue recover when encountering recovered Blues at rate η.

The value of Z changes according to different rates of attrition (β_U, β_D), and uses Lanchester aimed-fire model (2.1, 2.2). The value of B changes depending on kinetic effects and on epidemic effects according to the S-I-R epidemic model (2.5- 2.7). In this original model, Red is subject to aimed fire from all Blue units, and Blue is subject to aimed fire and cyber attack by Red. Only the Red force has cyber attack capability, and the asymmetry in capability of forces simplifies the analysis.

B. EXPANDED CYBER EPIDEMIC COMBAT MODEL DEVELOPMENT

Building upon this initial cyber epidemic combat model, we want to explore the interactions and implications for the clash of two cyber-capable sides, such that each side can degrade kinetic capabilities of the adversary using a cyber infection. We propose to use *two-sided* kinetic and cyber epidemic combat models; in order to understand the impacts on the battle of two fighting forces with both having asymmetric capabilities.

1. Two-sided Cyber Epidemic Combat Model

We start with generalizing the Schramm and Gaver (2013) model such that both sides have kinetic and cyber capability. This is the base model for us, which assumes aimed fire. The subscript *B* represents variables and parameters related to Blue force. The subscript *Z* represents variables and parameters related to the Red force.

For simplicity, suppress the explicit time-dependence notation, e.g., $S_B = S_B(t)$

B : level of Blue force at time *t*
Z : level of Red force at time *t*
ξ_B : Infection spread rate within B
η_B : Infection patch rate within B
ξ_Z : Infection spread rate within *Z*
η_Z : Infection patch rate within *Z*
ρ_U, ρ_D : Normal attack rate, and decreased (by infection) attack rate of *Z on B*
β_U, β_D : Normal attack rate, and decreased (by infection) attack rate of *B on Z*

The model equations are as follows:

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B - \eta_B S_B R_B) - [\rho_U(S_Z + R_Z) + \rho_D\,(I_Z)]\,\frac{S_B}{S_B + I_B + R_B} \quad (4.5)$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \eta_B I_B R_B) - [\rho_U(S_Z + R_Z) + \rho_D\,(I_Z)]\,\frac{I_B}{S_B + I_B + R_B} \quad (4.6)$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B) - [\rho_U(S_Z + R_Z) + \rho_D\,(I_Z)]\,\frac{R_B}{S_B + I_B + R_B} \quad (4.7)$$

$$\frac{dS_Z}{dt} = (-\xi_Z S_Z I_Z - \eta_Z S_Z R_Z) - [\,\beta_U(S_B + R_B) + \beta_D\,(I_B)]\,\frac{S_z}{S_Z + I_Z + R_Z} \quad (4.8)$$

$$\frac{dI_Z}{dt} = (+\xi_Z I_Z\, S_Z - \eta_Z I_Z\, R_Z) - [\,\beta_U(S_B + R_B) + \beta_D\,(I_B)]\,\frac{I_z}{S_Z + I_Z + R_Z} \quad (4.9)$$

$$\frac{dR_Z}{dt} = (+\eta_Z R_Z S_Z + \eta_Z R_Z I_Z) - [\,\beta_U(S_B + R_B) + \beta_D\,(I_B)]\,\frac{R_z}{S_Z + I_Z + R_Z} \quad (4.10)$$

Cyber Effects — Unaimed Degradation

Kinetic Effects — Aimed Fire Attrition

Fraction of Kinetic Effect

The first part of each equation represents the cyber effects on the total change of the number of units in a state, using an S-I-R epidemic spread . The second part of the equation, represents the kinetic effects on the depletion, using aimed-fire. This focuses proportionately on opposing units on each cyber-affected state.

We use the Lanchester aimed-fire model on kinetic battles unless stated otherwise. A modified SIR disease-spread model, as Schramm and Gaver (2013) describes the cyber effect. We make several assumptions. First, kinetic effects are assumed to be homogenous for each opposing force; each live unit has its own chance (probability) to survive in aimed-fire. Second, we assume there is only one vulnerability in each unit to exploit and

to patch (i.e., there is only a single type of infection). Third, we assume that infected units can be cured without any permanent damage, and return to original strength. Finally, we assume that both the kinetic battle and cyber operations (as represented by the infection) start at time $t = 0$.

The measure of effectiveness (MOE) is the number of killed target units for each opponent, unless stated otherwise

A visual summary of interactions and parameters in this model appears in Figure 9. In this figure alive Blue units can be in one of three states: S_B, I_B, R_B. Attrition from Blue goes to the (killed) state K_B. So S_B, I_B, R_B, K_B and B are all dynamic in nature, but they all sum up to a constant, B_0, the initial force size of Blue force. Specifically we have $B = S_B + I_B + R_B$ and $B_0 = B + K_B$. Analogous mechanics govern Red force dynamics, represented in terms of Z. **Note that this figure shows only positive values. Signs can be determined by the direction of the flow.**

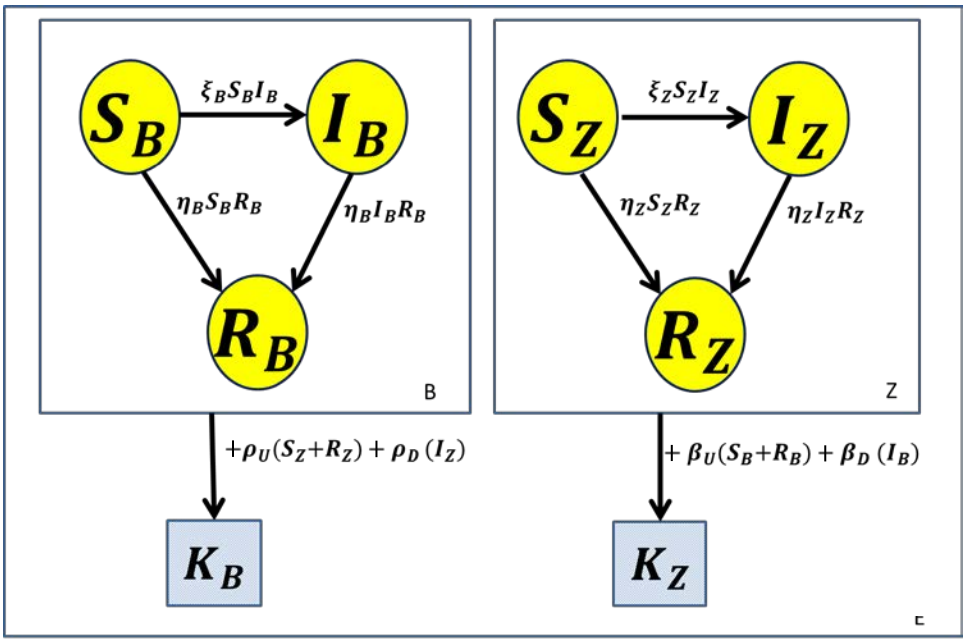

Figure 9. A two-sided Cyber Epidemic Combat model (General). Members of the Blue force (B) are in one of four states: susceptible (S_B), infected (I_B), recovered (R_B), or killed (K_B). Members of the Red force (Z) are represented similarly. Changes in states are represented by directed arrows, and the flow in *dt* is represented near arrows.

In the two-sided Cyber Epidemic Combat model, although attrition rates associated with infected or non-infected units are constant ($\rho_U, \rho_D, \beta_{U,} \beta_D$), the overall attrition rate is a weighted average of these constants, and the weights change with time. Table 1, displays the attrition rates.

Overall change in force (Attrition)	Without cyber effects	With cyber effects
$\frac{dB}{dt}$	$-\rho_U\, Z$	$-\rho_U\,(S_Z + R_Z) - \rho_D\,(I_Z)$
$\frac{dZ}{dt}$	$-\beta_U\, B$	$-\beta_U\,(S_B + R_B) - \beta_D\,(I_B)$

Table 1. The attrition rates with and without the cyber effects.

2. Compact Form of Two-sided Cyber Epidemic Combat Model

A more compact form to represent the same model can be stated using the overall change. Appendix C discusses about the use of this representations in cyber epidemic combat model. We use (4.11) as (4.5)+(4.6)+(4.7), and (4.12) as (4.8)+(4.9)+ (4.10).

$$\frac{dB}{dt} = -\rho_U(S_Z + R_Z) - \rho_D\,(I_Z)\,, \qquad (4.11)$$

$$\frac{dZ}{dt} = -\beta_U(S_B + R_B) - \beta_D\,(I_B)\,, \qquad (4.12)$$

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B - \eta_B S_B R_B) + \frac{dB}{dt}\frac{S_B}{B}, \qquad (4.13)$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \eta_B I_B R_B) + \frac{dB}{dt}\frac{I_B}{B}, \qquad (4.14)$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B) + \frac{dB}{dt}\frac{R_B}{B}\,, \qquad (4.15)$$

$$\frac{dS_Z}{dt} = (-\xi_Z S_Z I_Z - \eta_Z S_Z R_Z) + \frac{dZ}{dt}\frac{S_z}{Z}\,, \qquad (4.16)$$

$$\frac{dI_Z}{dt} = (+\xi_Z I_Z\, S_Z - \eta_Z I_Z\, R_Z) + \frac{dZ}{dt}\frac{I_z}{Z}\,, \qquad (4.17)$$

$$\frac{dR_Z}{dt} = (+\eta_Z R_Z S_Z + \eta_Z R_Z I_Z) + \frac{dZ}{dt}\frac{R_z}{Z}\,. \qquad (4.18)$$

C. MIXED EPIDEMIC COMBAT MODEL EXPLORATION

Begin by exploring the equations that represent the change in kinetic attack rate caused by cyber attack. Because cyber attacks and kinetic attacks have one common factor, and that is kinetic attack rate, cyber attack does not affect the battle with any effect except the effect on attack rate. Explaining the effects of cyber offensive and cyber defensive measures on kinetic attack rate would present insights about the overall picture. We continue with numerical explorations for each analytic discussion.

1. Attack Rates

The attack rate of Blue and the attrition rate of Red can be represented as:

$$\frac{dZ(t)}{dt} = -\beta_U \ [S_B(t) + R_B(t)] \ - \ \beta_D \ I_B(t)\,,$$

$$= -\beta_U \ [B(t) - I_B(t)] \ - \ \beta_D \ I_B(t)\,,$$

$$\equiv -\beta(t) \ B(t)\,,$$

where

$$\beta(t) = \frac{+\beta_U \ B(t) \ - \ \beta_U \ I_B(t) + \ \beta_D \ I_B(t)}{B(t)}.$$

Or:

$$\beta(t) = \ \beta_U - \frac{I_B(t)}{B(t)} \ (\beta_U - \beta_D)\,,$$

$$\beta(t) = \beta_U - I_B^{\alpha}(t) \ \ (\beta_U - \ \beta_D). \qquad (4.19)$$

Here, I_B^{α} is equal to the fraction of units in *B* that are infected at time *t*, and is scaled between 0 and 1. In addition, I_B^{α} is dynamic, so $\bar{\beta}$ (or $\beta(t)$) is a function of time, but we suppress time-dependency in notation for ease of display. We substitute $\bar{\beta} = \beta_U - I_B^{\alpha} \ (\beta_U - \beta_D)$, and $\bar{\rho} = \rho_U - I_Z^{\alpha}(\rho_U - \ \rho_D)$. In the representation $\beta_U - I_B^{\alpha}(\beta_U - \ \beta_D)$, the

attack rate of the Blue force is decreased with the proportion of infected in Blue, and the decrease in kinetic attack rate, based on the proposed model.

Attrition of Red can be modeled without any cyber infection effect on attacker as:

$$\frac{dZ}{dt} = -\beta_U B\ .$$

Now we can clearly see how a cyber infection in attacker units can affect attrition of the defender:

$$\frac{dZ}{dt} = -\beta_U\, B + (\beta_U - \ \beta_D)\, I_B. \qquad (4.20)$$

In words, a cyber infection of the Blue force (*B*) degrades the instantaneous attack rate on the Red force (*Z*) by an amount that depends on the number of infected Blue units at time *t* and the difference in attrition rates between the infected and non-infected units.

2. Cyber Operation Effects on Kinetic Attack Rates

We used the bar representation to clarify the effects on attack rates as in the previous section as:

$\bar{\beta} = \beta_U - I_B^{\alpha}\ (\beta_U - \beta_D)\ ,$

$\bar{\rho} = \rho_U - I_Z^{\alpha}\ (\rho_U - \ \rho_D)\ ,$

$$\frac{dB}{dt} = \ -\bar{\rho}\ Z\ , \qquad (4.21)$$

$$\frac{dZ}{dt} = \ -\bar{\beta}\ B\ . \qquad (4.22)$$

We can summarize these effects in Table 2.

Overall change in force (Attrition)	Without cyber effects	With cyber effects
$\frac{dB}{dt}$	$-\rho_U\ Z$	$-\bar{\rho}\ \ Z$
$\frac{dZ}{dt}$	$-\ \beta_U\ B$	$-\bar{\beta}\ \ B$

Table 2. The change in models with and without the cyber effects, simplified.

A visual representation of the states and the parameters can be summarized as in Figure 10.

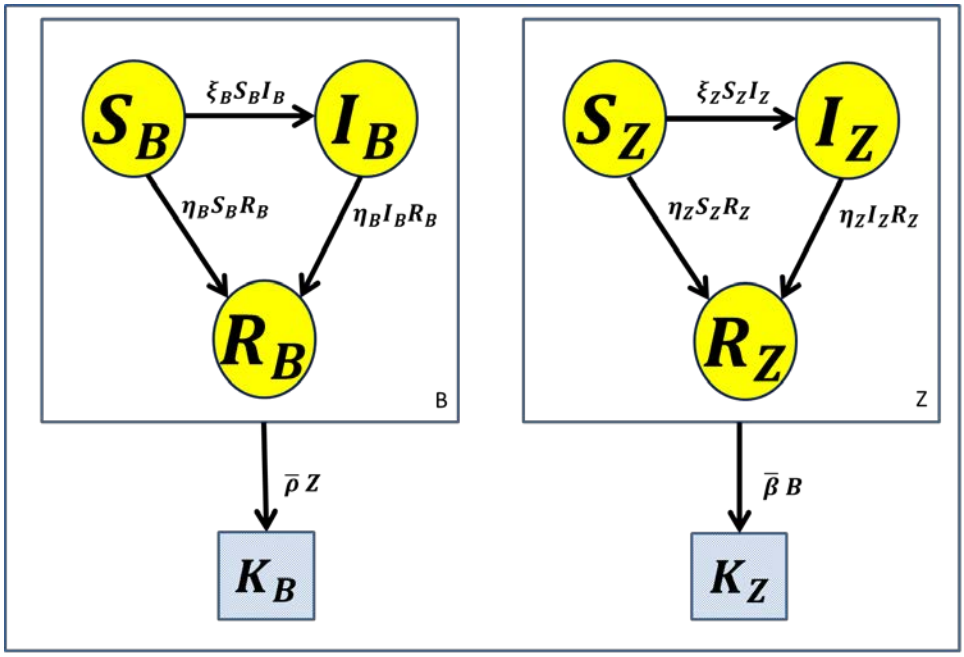

Figure 10. A two-sided Cyber Epidemic Combat model.

Figure 11 represents the model without any cyber effect. So comparison of Figure 10 and Figure 11 shows how the cyber effect changes the model.

Figure 12 represents the model with cyber degraded attack rates. Thus, Figure 10 and Figure 12 are essentially the same. Comparing these two figures reveals how the underlying mechanics work for cyber effects.

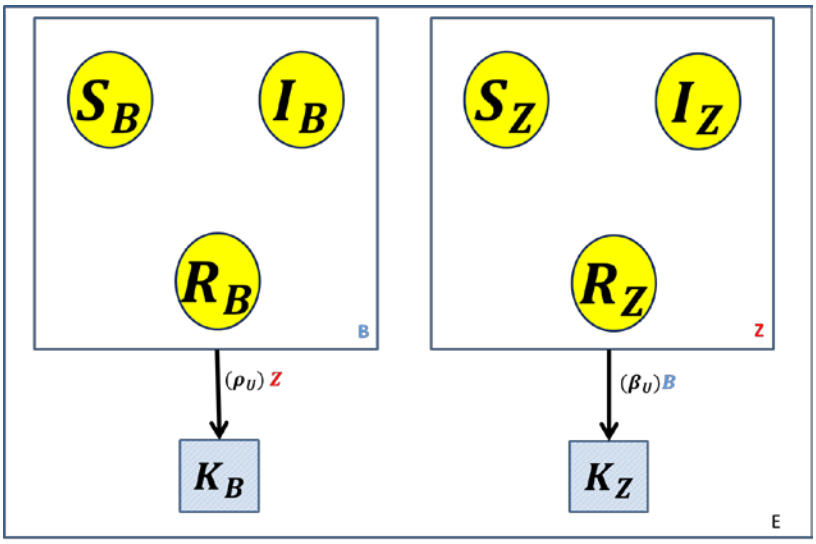

Figure 11. A Kinetic model without any cyber effects.

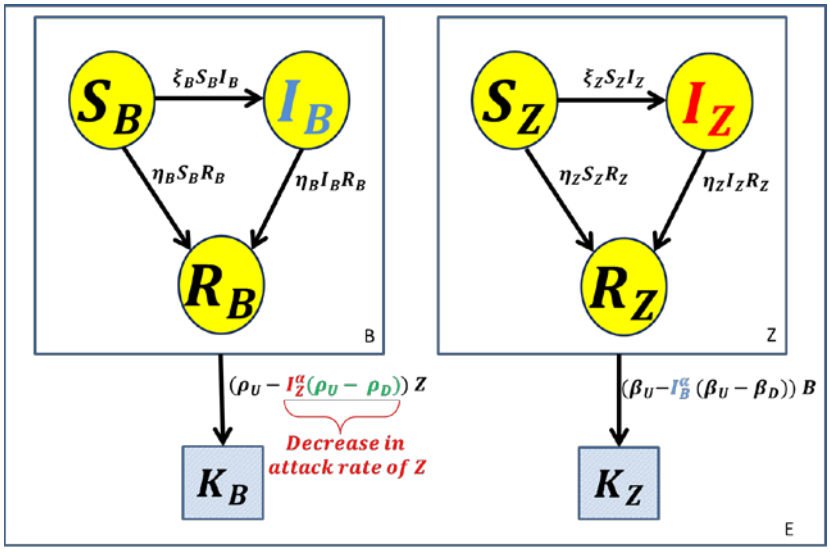

Figure 12. A Kinetic model with cyber effects.

These formulations reveal that the attack rate of Blue is decreased under cyber attack, in proportion to the ratio of infected Blue units to fighting Blue units and the difference of normal and decreased kinetic attack rate. This reinforces and quantifies the intuition that effectiveness of an infection (lower β_D) is as important as the spread capability of the infection. Similarly, any step to reduce the degradation of an infected unit is as important as any step to reduce the spread of the infection. On one hand, we assumed a constant decrease on the attack rate which causes a proportional decrease in cyber effect,

on the other hand, the spread of the infection accelerates with time, which causes the cyber effect to be more rapid initially. In this case, the spread speed of the infection has a dominant role.

3. Numerical Exploration for Various Parameter Values

We will now use our model to explore how forces behave with and without cyber infection. In the figures that follow, bold lines represent number of Blue and Red units (and total attritions). Note that, we increased the detail level in the graphs by using 10 steps in 1 time (t), **and to reproduce these figures, time should be divided by 10.**

We begin with the simple case where both sides are symmetric in initial size and capability. Figure 13 shows the Lanchester dynamics for a conventional aimed-fire battle without any cyber effect, along with a complete replication of model parameters. The dynamics display a conventional aimed-fire pattern. Because the two sides are symmetric, Red and Blue Forces annihilate one another.

We next consider the case where only one side has a cyber capability (equivalently, the other side is the only one that suffers from a cyber infection). In Figure 14 one side (Red) has one cyber-infected unit initially, and there is asymmetry in the initial conditions of the conventional combat. We can see how the cyber effect changes the total force sizes of Blue and Red.

Figure 13 and Figure 14 clearly shows that a single infected unit may have a large effect on the battle outcome.

Of course, it is not the presence of a cyber capability alone that leads to victory, but that may be an advantage of one side over the other. Figure 16 shows the case where both sides have an identical cyber capability; in this case, the model parameters are symmetric, and the battle is again a draw.

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	950	***0***	50	0.10	0.01	0.0050	0.0005
Red	1000	950	***0***	50	0.10	0.01	0.0050	0.0005

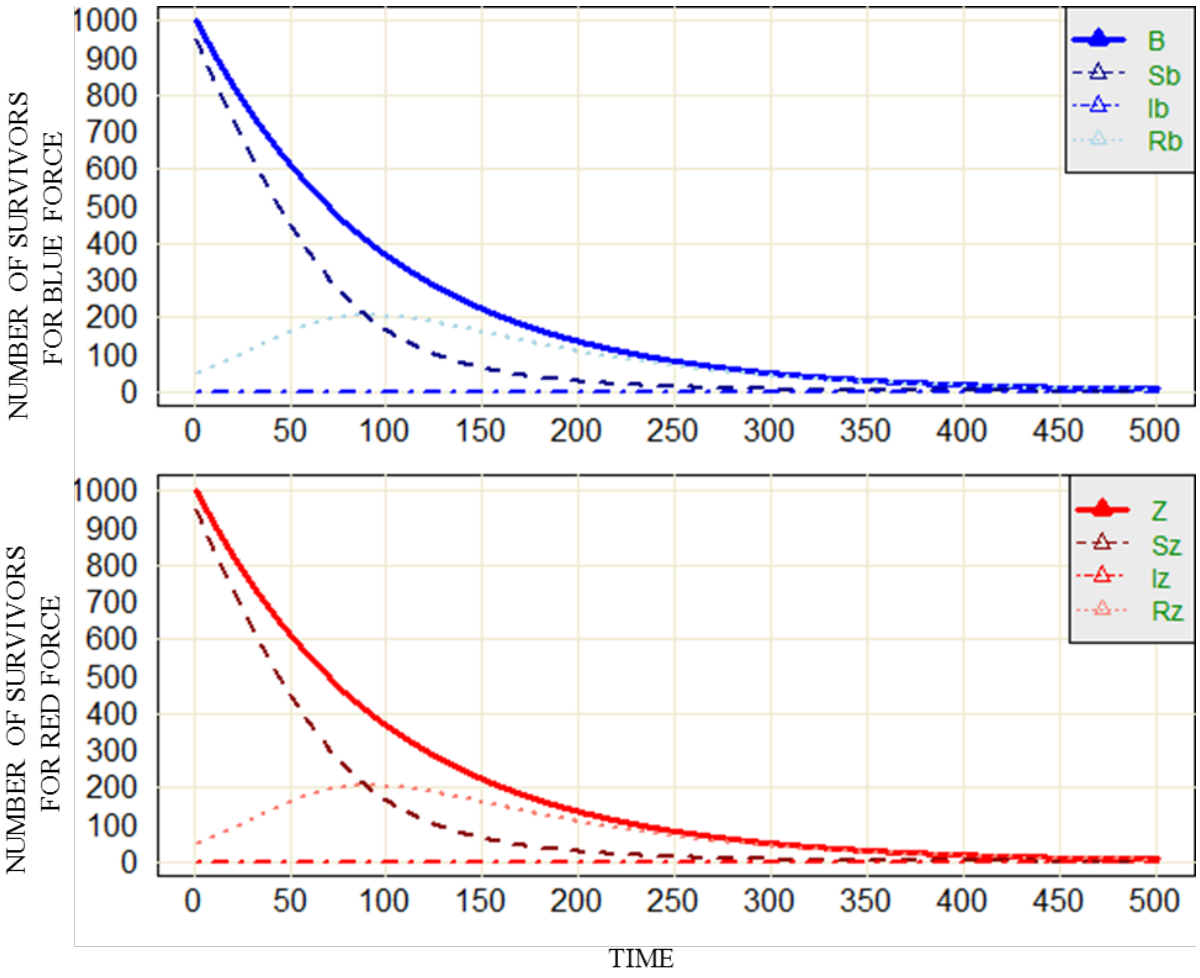

Figure 13. No initial infection of Blue or Red.

In this battle, initial parameters are the same for both sides. Since two sides are symmetric, Red and Blue annihilate one another. There is **no cyber effect** and the graph shows a conventional aimed-fire pattern. The battle result is a draw. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	950	***0***	50	0.10	0.01	0.0050	0.0005
Red	1000	949	***1***	50	0.10	0.01	0.0050	0.0005

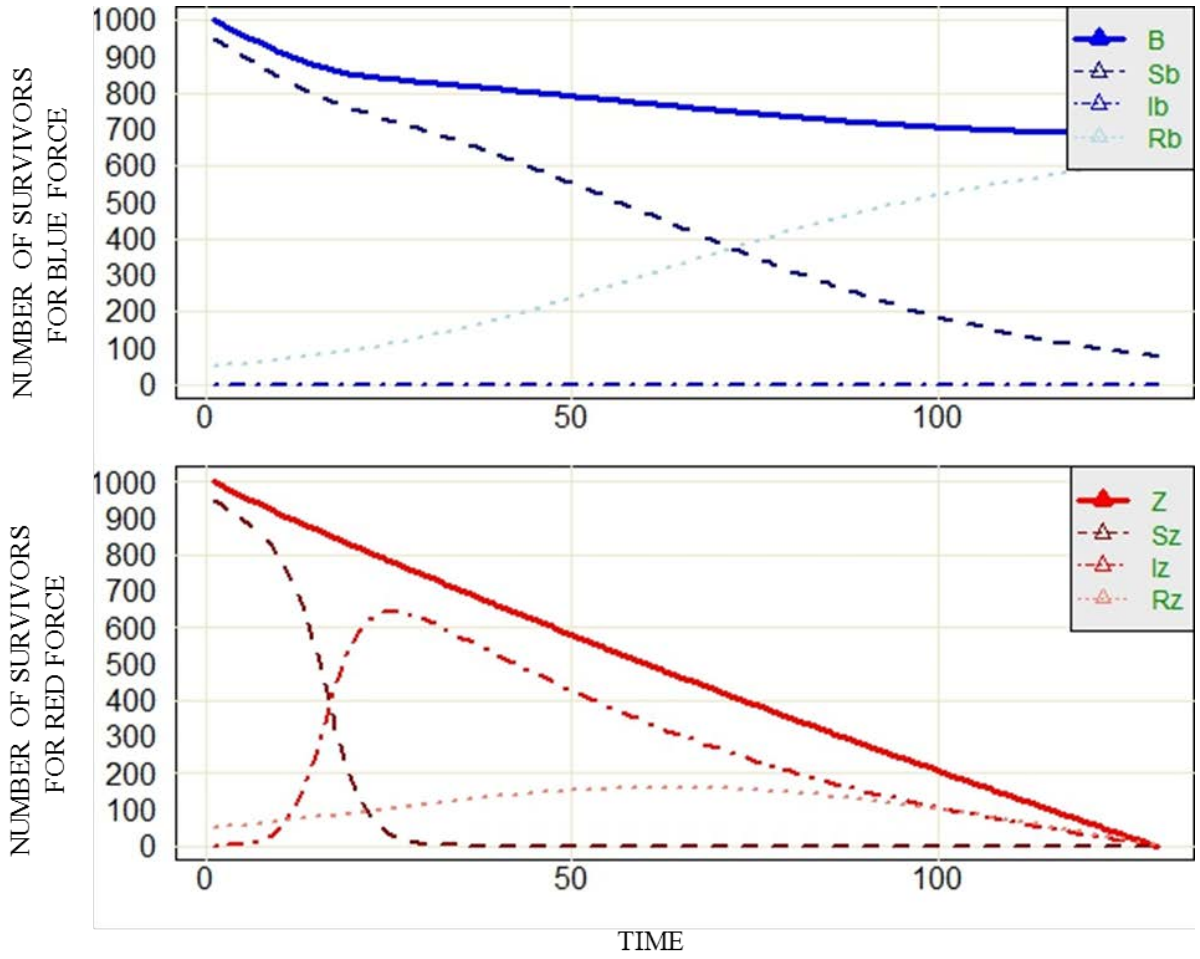

Figure 14. Minimal initial infection on one side, Red.

In this battle, initial parameters are the same except the number of infected. So, we can see the change in number of units when two equal (symmetric) forces fight, and one side (Red) is infected. The battle results in clear victory of Blue. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	***1***	50	0.10	0.01	0.0050	0.0005
Red	1000	949	***1***	50	0.10	0.01	0.0050	0.0005

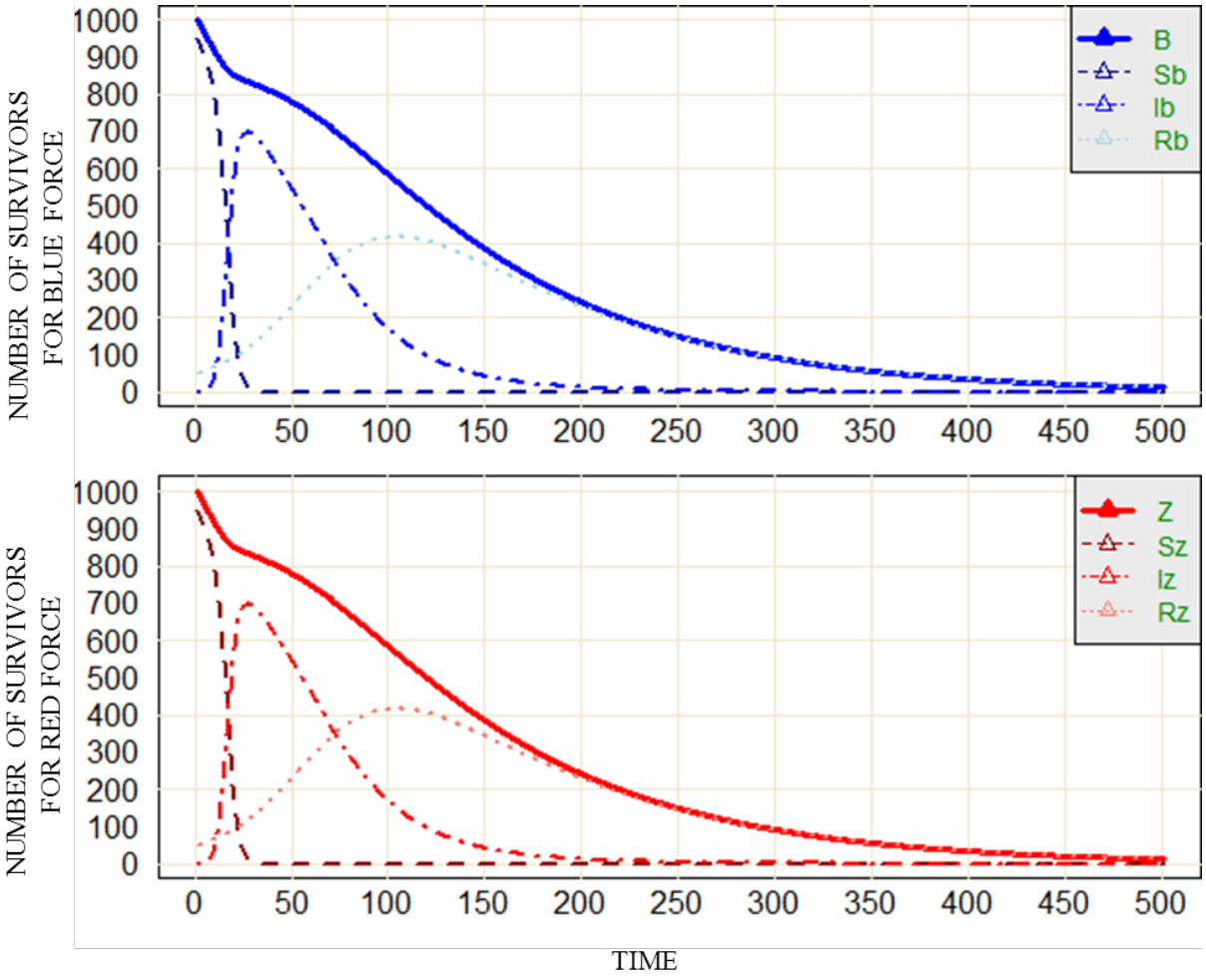

Figure 15. Minimal initial infection on both sides.

In this battle, initial parameters are **the same for both sides**, again. Two sides are symmetric, Red and Blue annihilate one another, but the graph shows a different pattern from a conventional aimed-fire. The difference is caused by the infections on both sides. (Time is multiplied by 10.)

A larger initial infection on one side accelerates the overall infection process and limits even more the fighting capability of that infected side. Figure 16 shows the case where $I_Z = 50,$ and there are fewer susceptibles (so the overall population size remains constant). Figure 17 shows the similar case where $I_Z = 500,$ all other conditions being equal. Although the infection happens faster, the overall battle time does not change significantly, and the results are qualitatively the same.

Figure 18 considers the case where the initial infection is symmetric, i.e., $I_B = I_Z = 1,$ but where one force (Red) has a larger number of susceptibles, and therefore an overall larger force size. In this case, the advantage in a larger initial force size gives Red the victory, despite the fact that a larger force is a larger target. Greater disparity in the initial sizes of Blue and Red, as shown in Figure 19, makes the result even more dramatic. Specifically, we observe that between Figure 18 and Figure 19 there is about 9% difference in force for initial conditions. However, the results of the battle changed in favor of Red by 20%. This is because of the very nature of aimed fire.

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	950	**0**	50	0.10	0.01	0.0050	0.0005
Red	1000	***900***	***50***	50	0.10	0.01	0.0050	0.0005

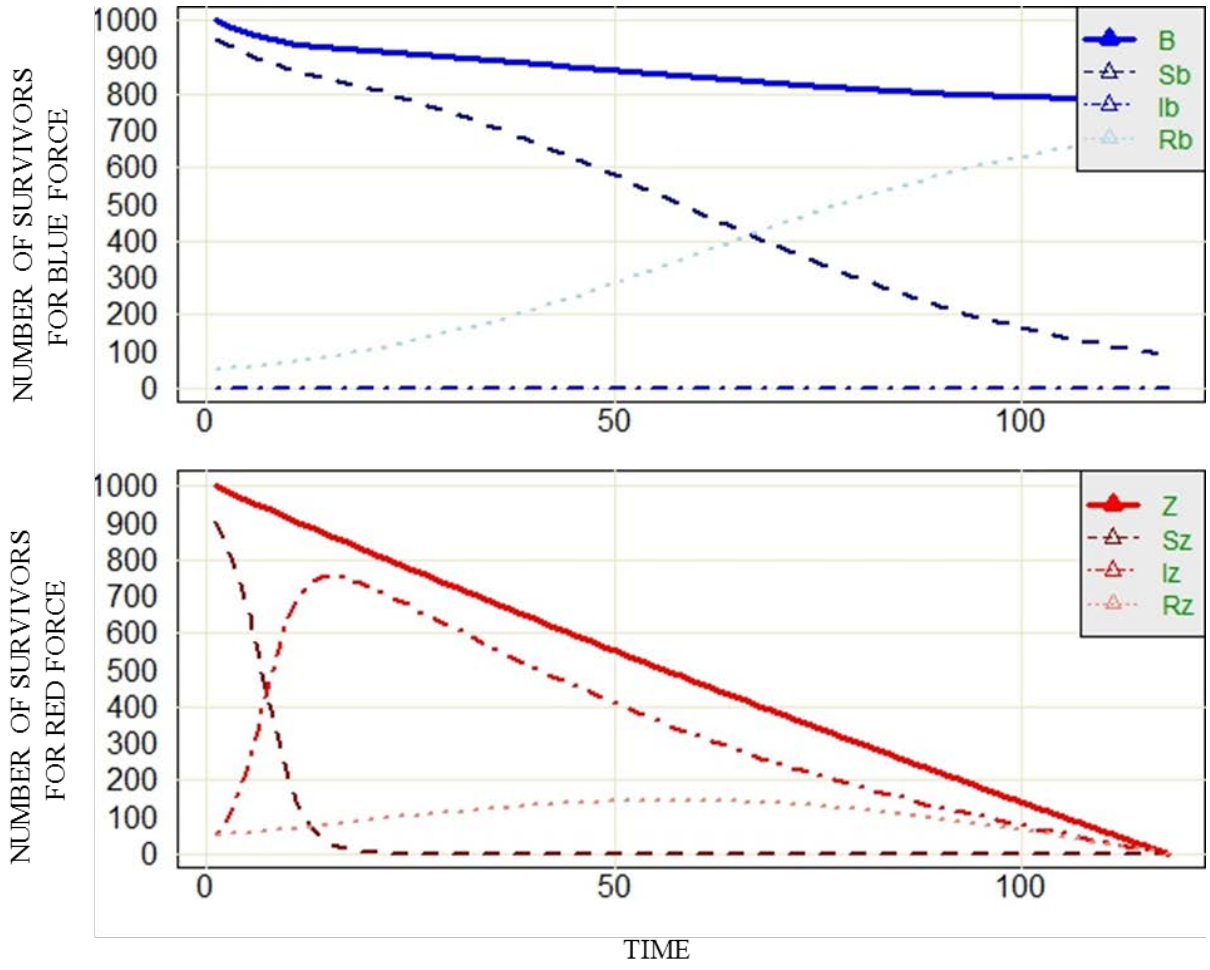

Figure 16. Increased initial infection on Red, (50x).

In this battle, initial parameters are the same except for the number of infected Red. We increased the number of infected by 50 times to see the difference. We see that Blue wins, but the increase does not change the outcome or time of battle significantly. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	950	***0***	50	0.10	0.01	0.0050	0.0005
Red	1000	***450***	***500***	50	0.10	0.01	0.0050	0.0005

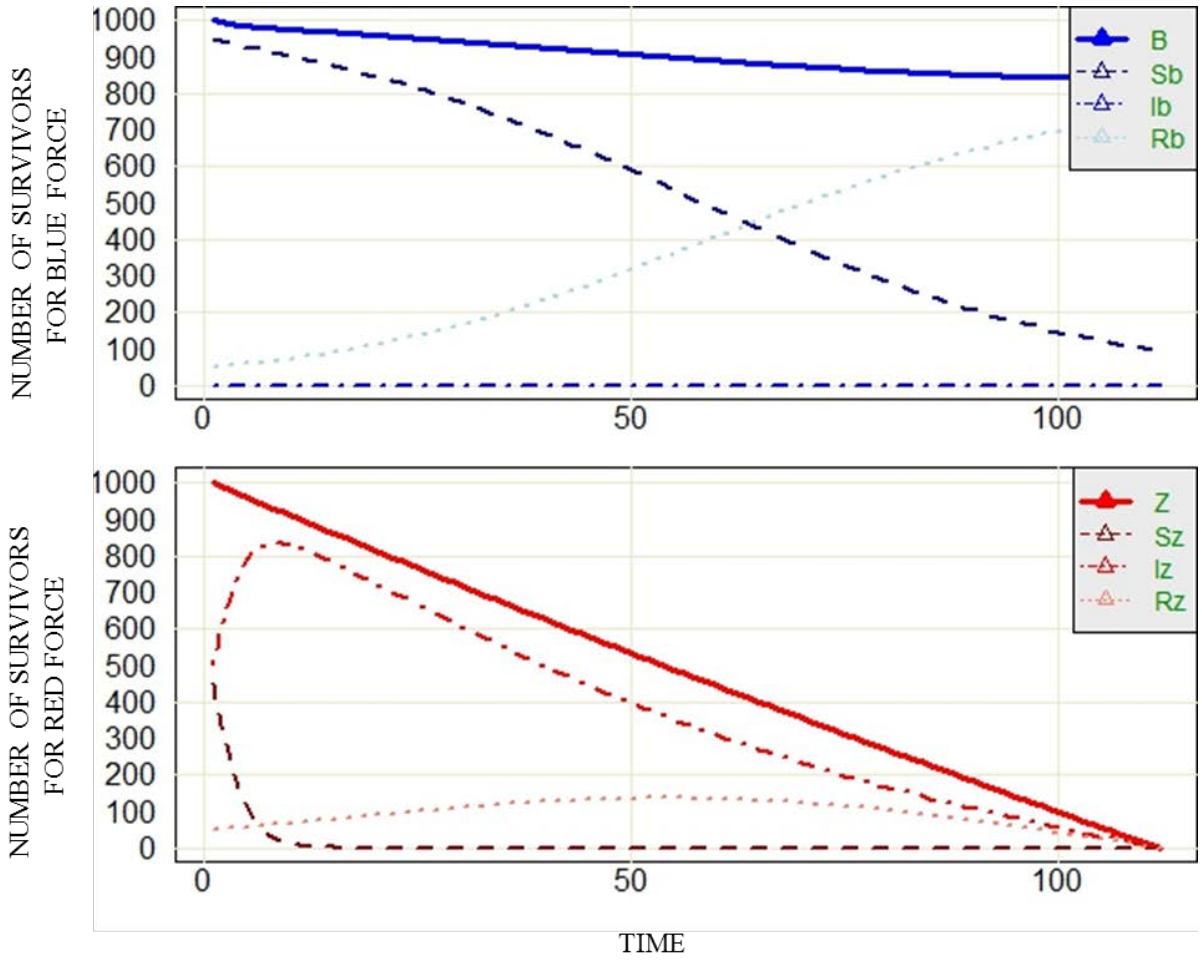

Figure 17. Increased initial infection on Red, (500x).

In this battle, initial parameters are the same except the number of infected. In the case where the number of infected is increased 500 times, we see that Blue wins again, but the increased level in infected, the outcome, and time of battle does not change significantly. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (*B*, *Z*)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	***1051***	***1000***	1	50	0.10	0.01	0.0050	0.0005

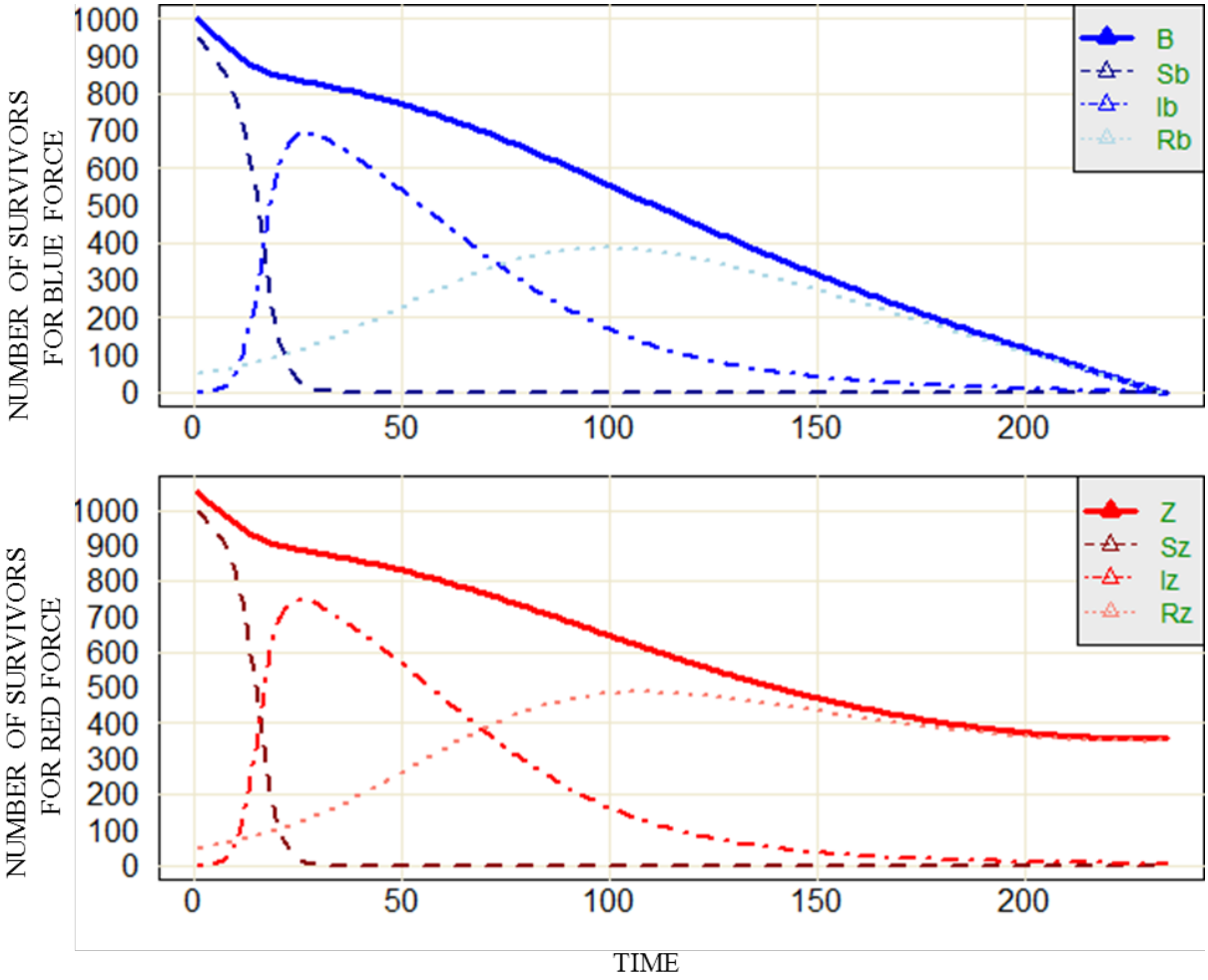

Figure 18. Increased initial susceptibles on Red (5%).

In this battle, initial parameters are the same with infection, for both sides. We increase the initial number of susceptibles (and overall unit number) for Red by 5%. The difference in outcome caused by this increase is about 40% of initial, and is significantly higher than the input resource. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	***1131***	***1080***	1	50	0.10	0.01	0.0050	0.0005

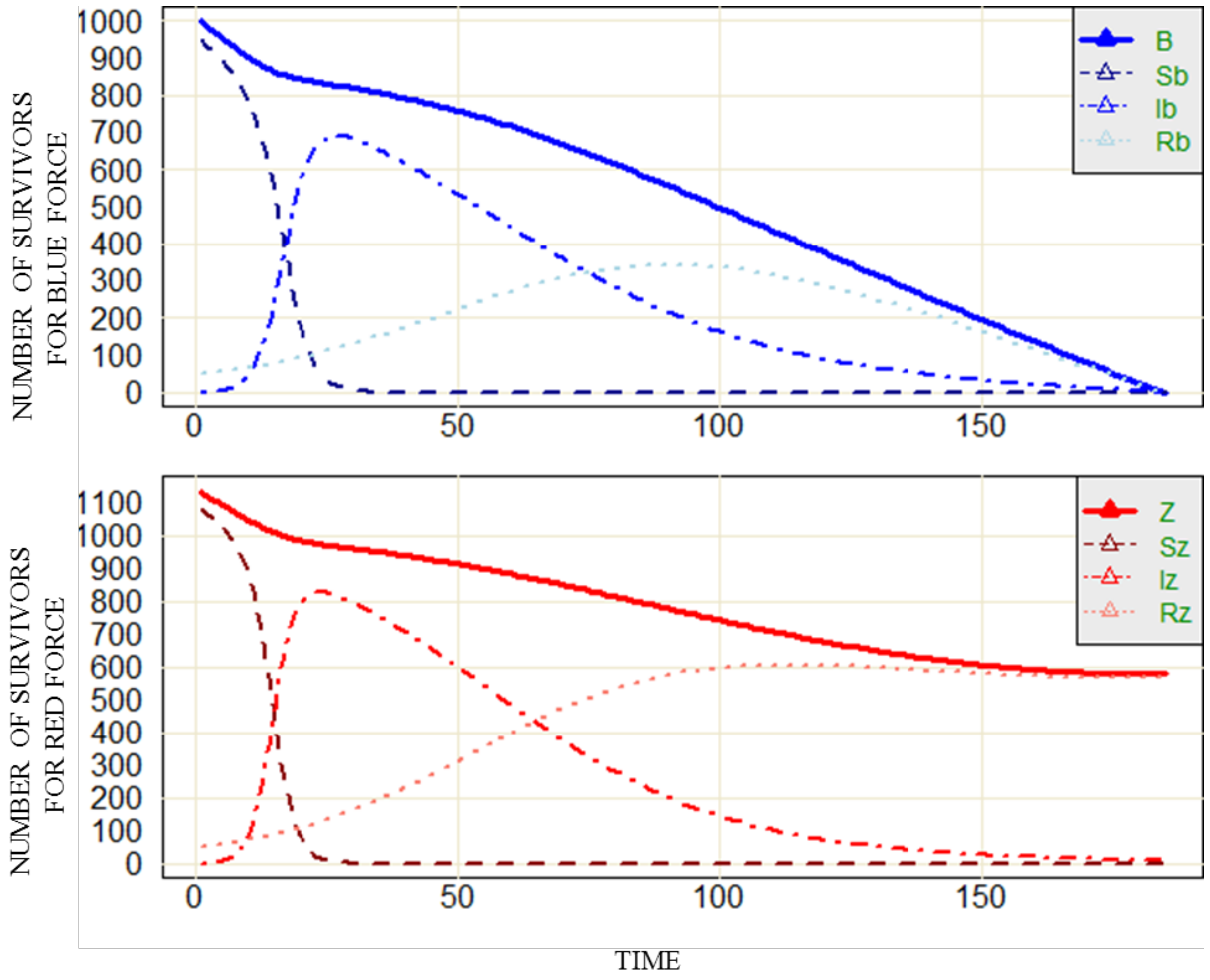

Figure 19. Increased initial susceptibles on Red (13%).

In this battle, to compare with Figure 18, we increase the initial number of susceptibles (and overall unit number) for Red by 13%. The difference in outcome caused by this increase is about 60% of initial. The marginal effects of initial number of units are decreasing, but still significant. (Time is multiplied by 10.)

We use the scenario in Figure 19 (symmetric initial infections, but a larger fighting force for Red) to explore tradeoffs in other model parameters.

In Figure 20 we decrease the patch (recovery) rate from 0.0005 to 0.0003 (a 40% reduction) there is a significant change on the number of survivors. However, in Figure 21 when we decrease the patch rate from 0.0005 to 0.0002 (a 60% reduction), we see that the victorious side changes. As shown in Figure 22 with a patch rate of .0002788 (a 45% reduction), the outcome of the battle is a draw. So, overall a 45% decrease in patch rate has approximately the same effect as a 13% decrease in force level. We should note that these estimates are for given parameters on given points.

In Figure 23, we use the same method to see the effects of the spread rate, however, the effect of the spread rate is not very significant. The marginal effect of each additional infected unit (on the battle outcome) decreases as initial number of infected units increase, and after a point any addition to spread rate or initial infected unit does not affect (insignificant) the overall course of the battle. In this case comparing with Figure 19 increasing the spread rate by 160 times is not enough to change the victorious side,

In Figure 24 we try to get the same type of result as in Figure 22 by decreasing the initial number of recovered this time, by keeping the patch rates the same with Figure 19. We see that a 72% decrease in number of initial recovered units has the same effect as a 45% decrease in patch rates or 13% decrease in number of fighting units, for given set of parameters.

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	***1131***	***1080***	1	50	0.10	0.01	0.0050	***0.0003***

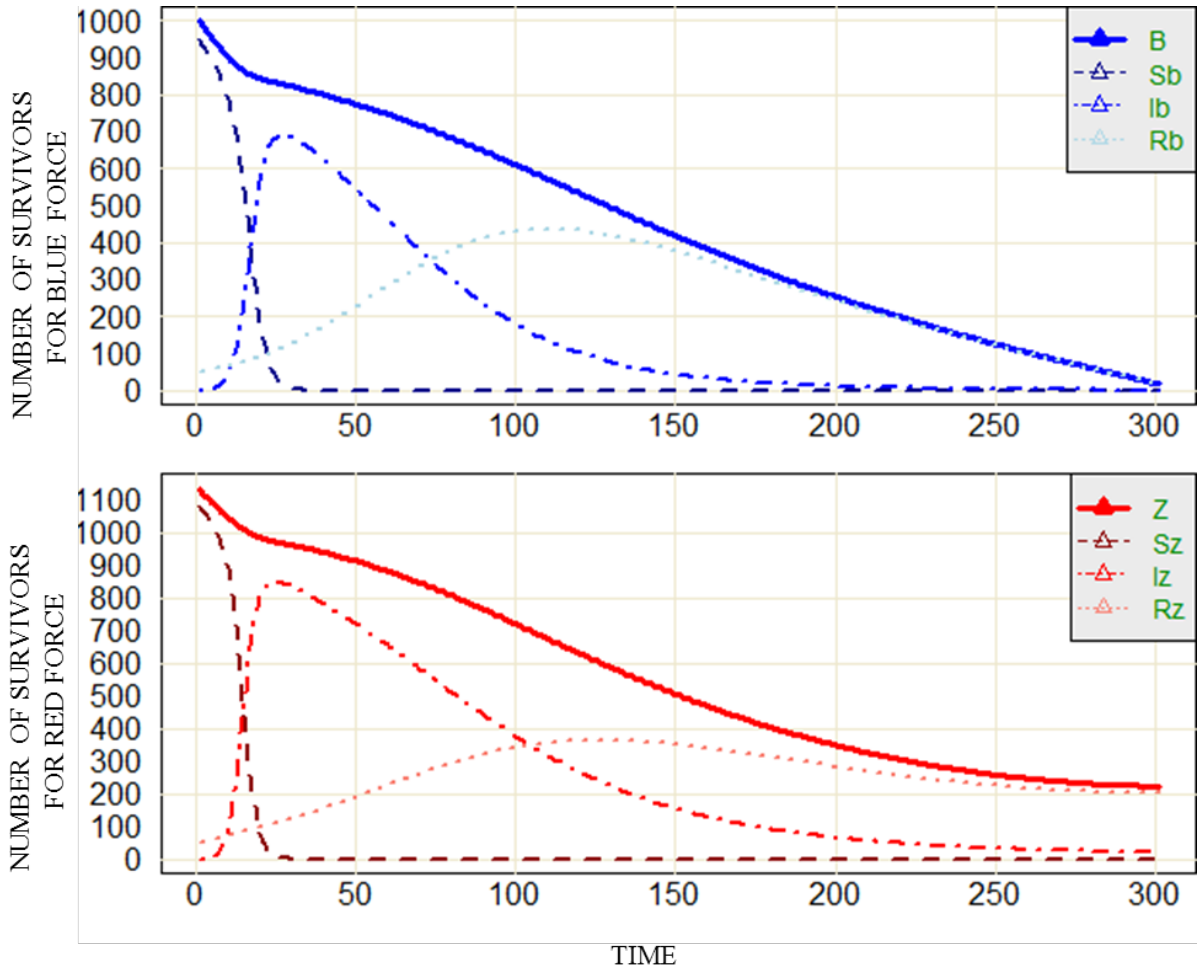

Figure 20. Increased initial susceptibles and 40% decreased patch rate within Red. In this battle, to compare with Figure19, we decrease the patch rate for Red by 40%. The difference in outcome caused by this decrease is about 40% of initial. We see that patch rate affects the overall course of the battle significantly. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (*B*, *Z*)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	***1131***	***1080***	1	50	0.10	0.01	0.0050	***0.0002***

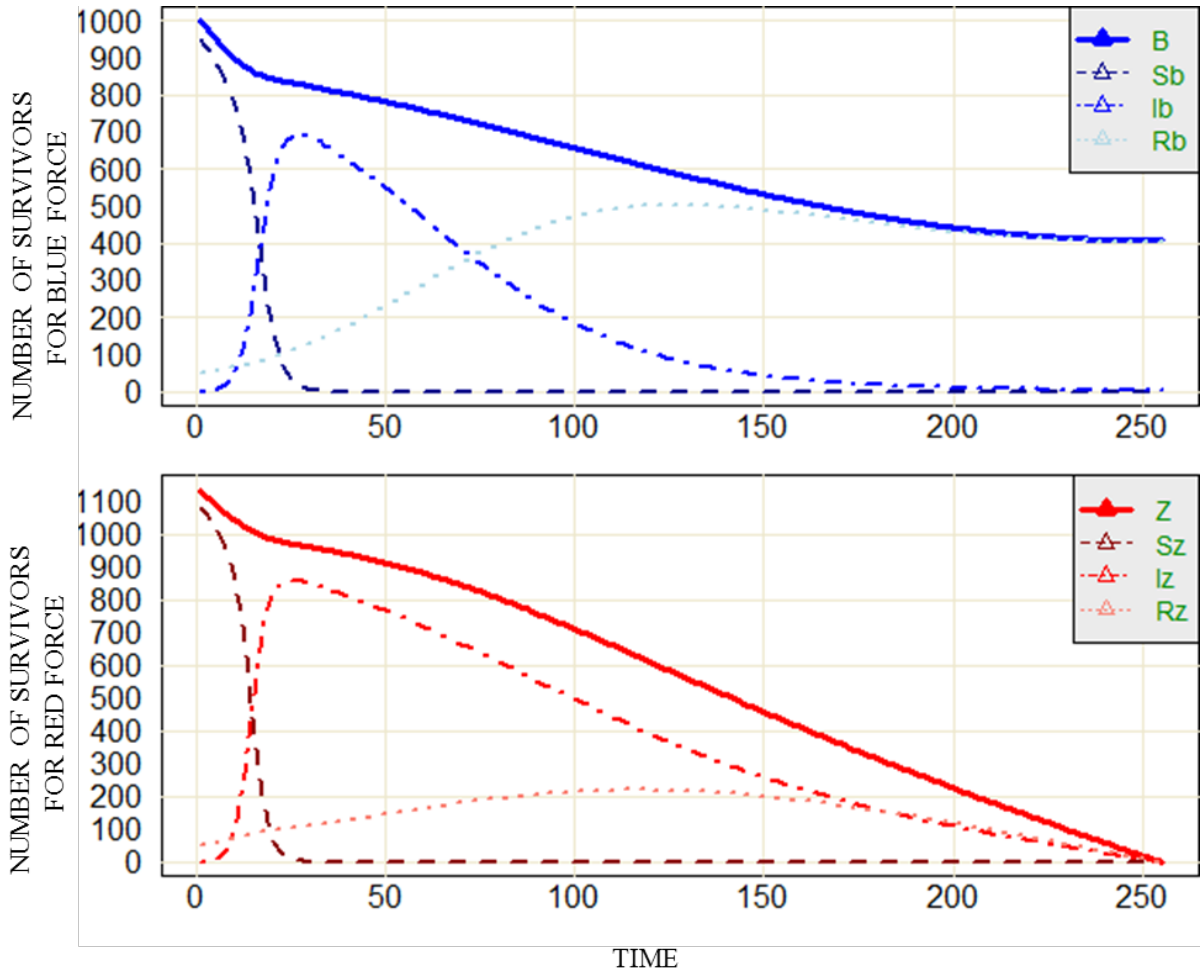

Figure 21. Increased initial susceptibles and decreased patch rate within Red.

In this battle, to compare with Figure 19, we decrease the patch rate for Red by 60%. **The difference in outcome caused by this decrease is very large**. We see that patch rate affects the overall course of the battle significantly. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (*B*, *Z*)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	***1131***	***1080***	1	50	0.10	0.01	0.0050	***.0002788***

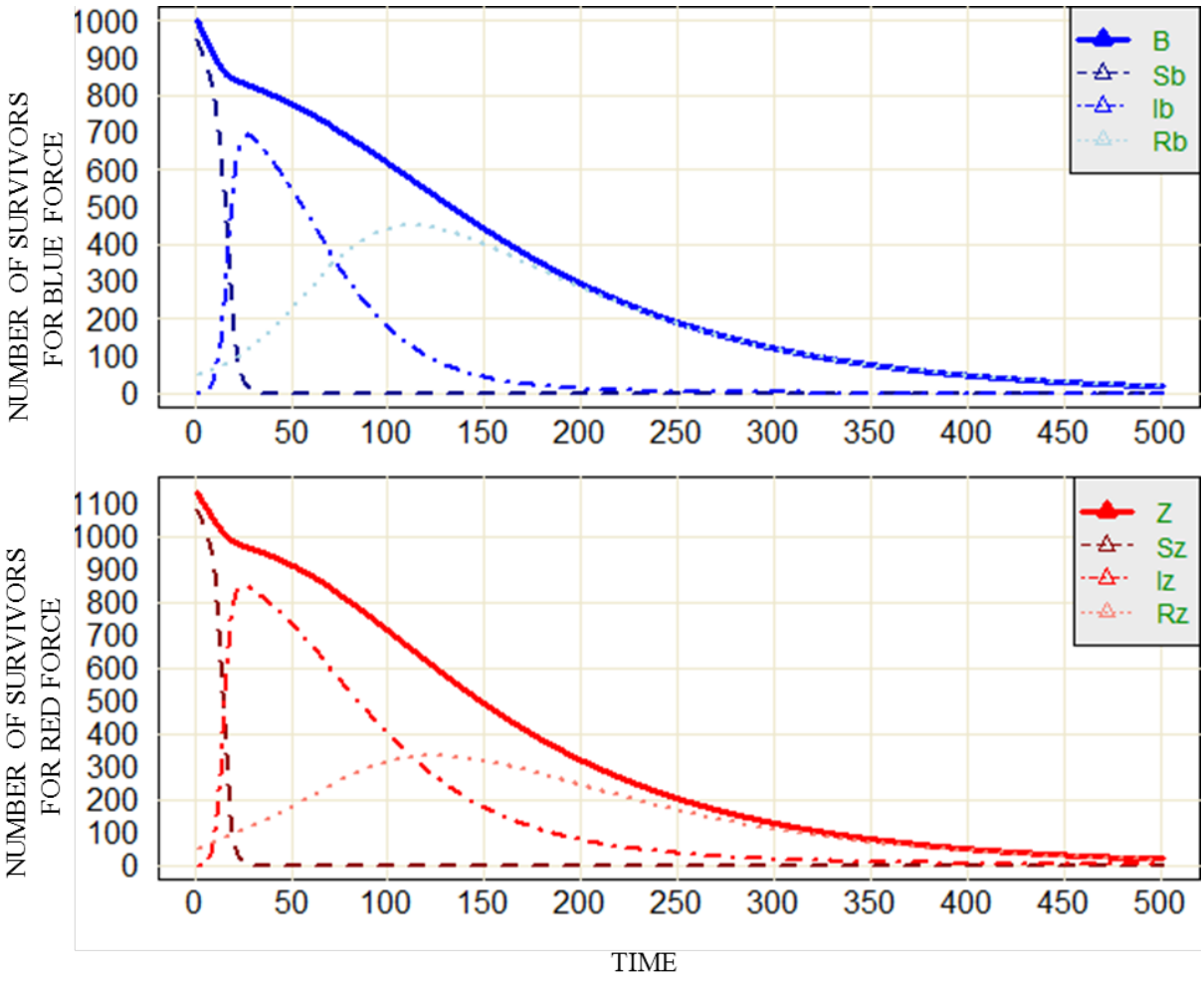

Figure 22. Increased initial susceptibles and decreased patch rate within Red. For this battle, we compare with Figure 15, because results are the same. Comparing to the initial symmetric battle, we increased the number of Red units by 13%, and decrease the patch rate for Red by 44%. The battle result is a draw again. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	***1131***	***1080***	1	50	0.10	0.01	***0.8000***	0.0005

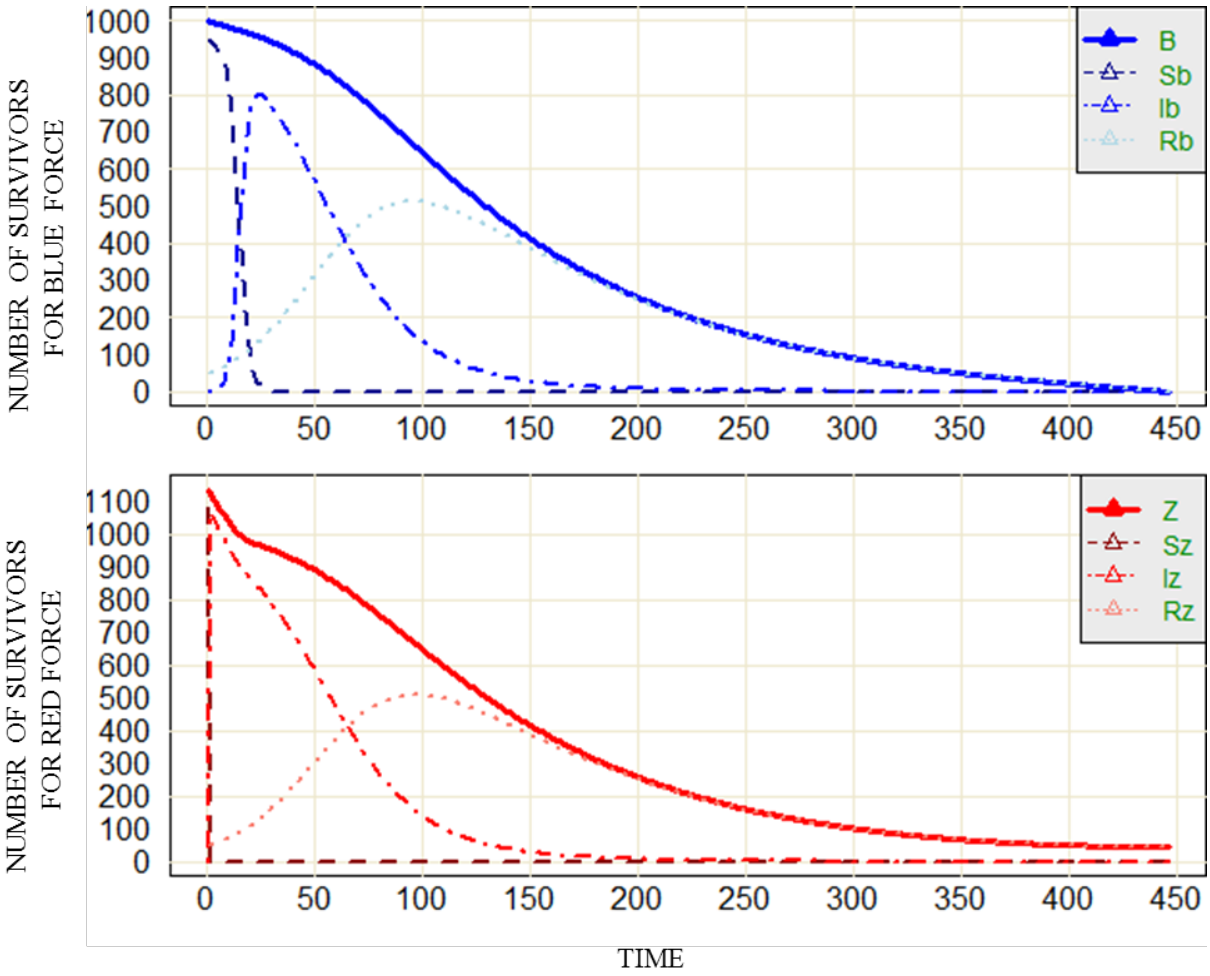

Figure 23. Increased initial susceptibles and increased spread rate within Red (160x). For this battle, we compare with Figure 15, because results are similar. Comparing to the initial symmetric battle, we increased the number of units by 13%, and increased the infection rate for Red by 160 times. The result is slightly in favor of Red. So, the spread rate does not affect as much as patch rate does in this case. (Time is multiplied by 10.)

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	***1131***	***1116***	1	***14***	0.10	0.01	0.0050	0.0005

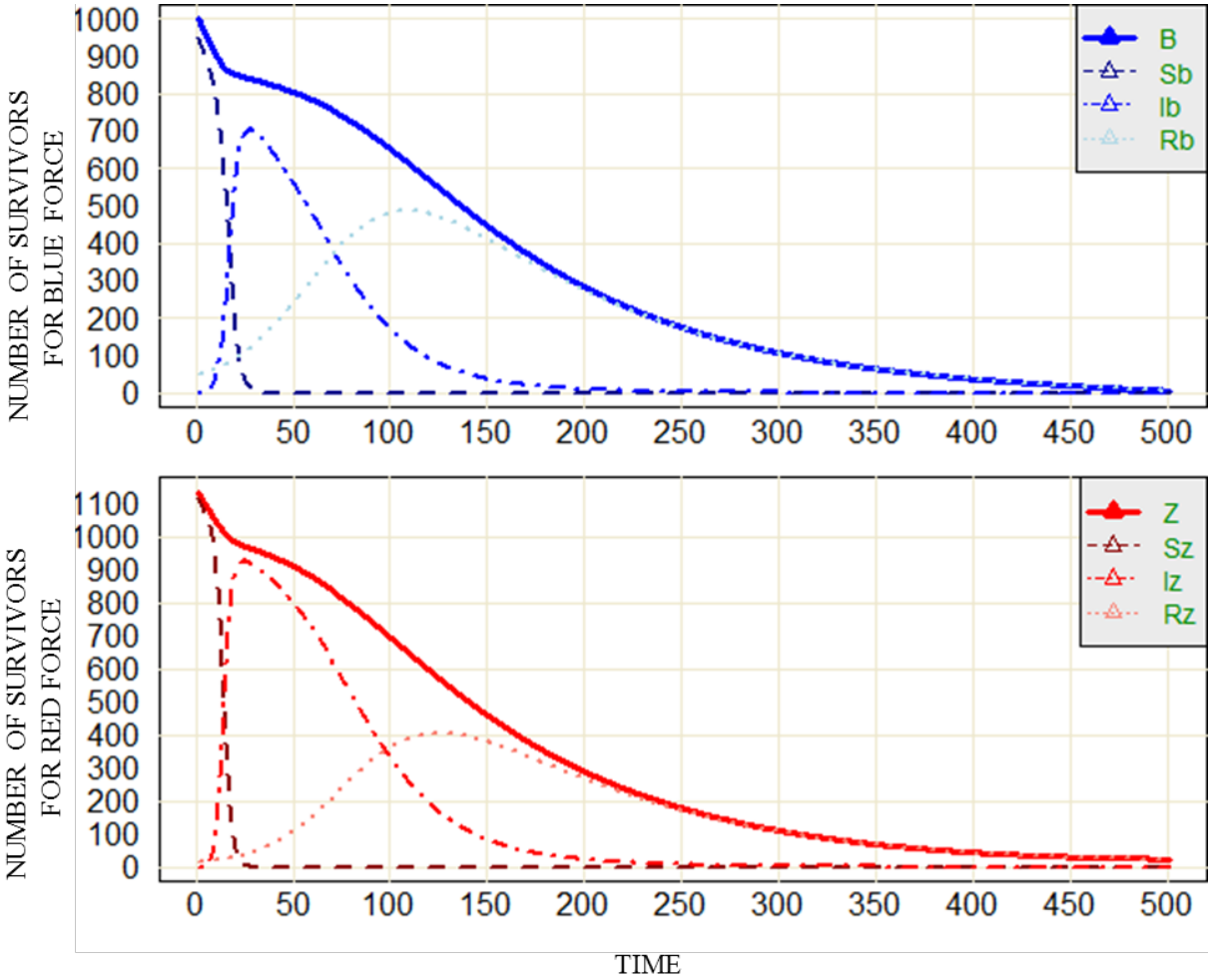

Figure 24. Increased initial susceptibles and decreased recovered on Red.

For this battle, we compare with Figure 15, because results are the same. Comparing to the initial symmetric battle, we increased the number of units by 13%, and decrease the initial number of recovered for Red by 72%. The battle result is a draw again. (Time is multiplied by 10.)

4. Numerical Exploration for Attack Rates

To solve the differential equations numerically, we used the programming language "R" (Ihaka and Gentleman, 1996) as the main software with the DeSolve Package (Soetaert et al., 2010) to estimate the point at which one side is annihilated (the root of one of the two equations). No step-size was declared for the solver. Due to the model structure, force numbers may go negative unless stopped at the zero boundary.

Attack rates are at the core of this study. It is the common parameter linking cyber and kinetic attacks. The victory is driven by the result of the kinetic battle, so by number of units ultimately. The result of a kinetic battle is driven by two sets: numbers of units, and attack rates. However, cyber attacks have no direct effect on number of surviving units, it just affects the attack rates. So cyber attacks can change the course of a battle by affecting the attack rates.

Attack rates are assumed to be constant in a kinetic-only battle, as in original Lanchester equations. Cyber operations cause these rates to fluctuate in time for the deterministic models. We have shown that the decrease in attack rate is directly related to the fraction of attacker units infected. We will further discuss how these fluctuations may affect victory conditions and how cyber operations can be a decisive action in a combat in Section IV.C.8.

We showed how cyber and kinetic attack rates can change by shock in Chapter III, in a discrete manner. This chapter explores the same content in a continuous manner. Thus, in Figure 25, we see how one cyber-capable side can change the attack rate of its adversary over time with the mixed epidemic combat model.

Figure 26 shows the change in attack rates when both sides have cyber attack capabilities, and gives a sample for the interaction between them.

Overall, in Figure 25 one side is infected, and in Figure 26 both sides are infected. The difference between Figure 25 and Figure 26 is what we explore in this chapter.

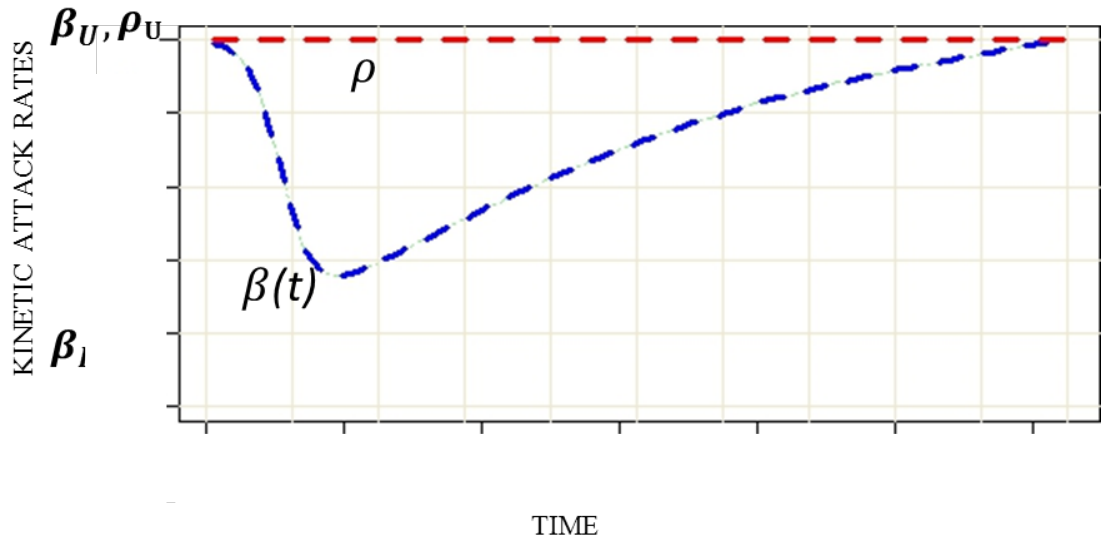

Figure 25. A notional attack rate graph, Blue is under infected by Red. Red is not infected.

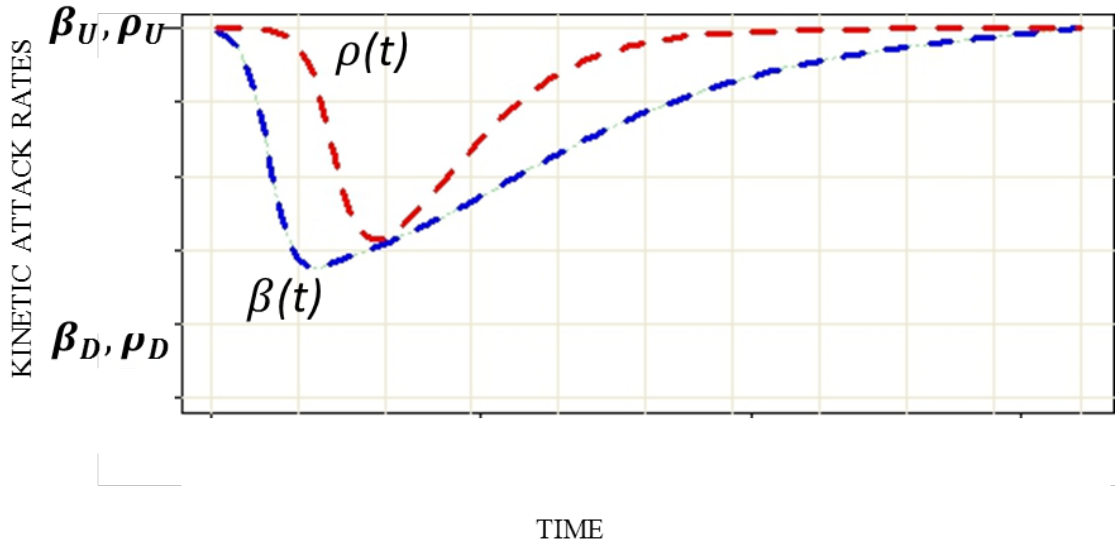

Figure 26. A notional attack rate graph, each side is infected by the other side.

In Figure 27 we can see that $\beta(t) = \beta_U - I_B^{\alpha}\ (\beta_U - \beta_D)$ was decreased by a cyber operation, and ρ is constant. Although Red here has a significantly lower attack rate (ρ), Blue attack rate $\beta(t)$ can be forced to be lower than ρ depending on other parameters.

With optimum cyber capabilities, Red can have attack rate superiority for long enough, which may lead to combat victory.

The underlying situation in Figure 27 is that although both forces start with the same number of units, Blue was infected by Red immediately after the battle starts. The infection spreads 10 times faster than it is cured in susceptibles, but Blue forces can patch both infected units and susceptibles. The infection decreases the kinetic attack capability to 10% of initial. The infection does not last more than 20% of the battle time when we run the model, but changes the result of the battle.

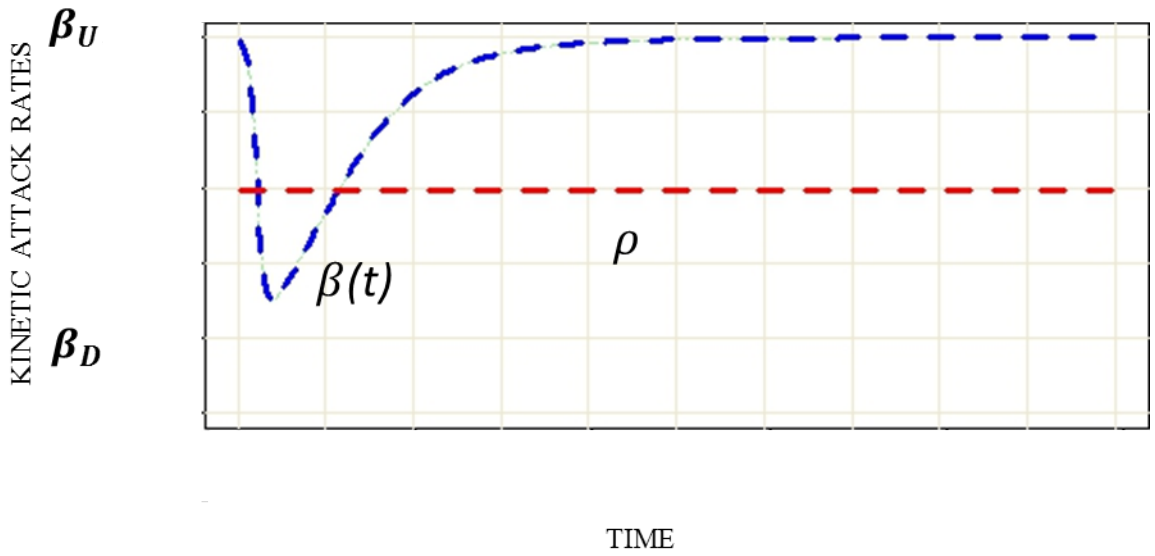

Figure 27. A notional attack rate graph, Blue is under cyber attack by Red. Number of initial units in this figure is the same. Although the initial kinetic attack rate of Blue is significantly higher than Red's attack rate, Blue is quickly infected by Red. The result of the battle is a draw.

5. Numerical Sensitivity Analysis of Parameters

To understand the effects of parameters on the overall battle result, we numerically conduct sensitivity analyses. Since the model uses several parameters, we fix each parameter and vary two of them each time to have a two-dimensional visual

representation. This approach restricts us to a very specific range, but may help to gain insight.

We represent blue color when Blue force wins, and red color when Red force wins. The parameters are fixed as Table 3 except two analyzed ones, which are specified in the figure. The parameters are symmetric unless stated otherwise. We display the results in Figure 29.

When comparing infection spread rates, ξ_B and ξ_Z, the result is intuitive. We use the range (0, 0.02) for both parameters, and because we assume two symmetric forces in the experiment, depending on two symmetric parameters, the graph is also symmetric. So if Blue force was infected by a more powerful infection, then the spread rate in Blue (ξ_B) would be higher, which would lead Red to win. The same conditions apply to Blue.

When comparing the infection spread rate of Blue, ξ_B,, and the patch (recovery) rate of Blue ,η_B , we observe a non-linear interaction for these two parameters. Using the range (0, 0.004) for η_B and (0, 0.04) for ξ_B, we see that η_B has a dominant effect over ξ_B. The underlying reason for this may be the marginal effect of ξ_B, which decreases when the spread rate ξ_B gets larger.

We also compare the infection spread rate of Blue, ξ_B, and the patch (recovery) rate of Red, $\eta_{Z,}$ and we see a different pattern. These two parameters may seem unrelated, but in a highly-interactive environment they should be. We use the range (0, 0.002) for η_Z and (0, 0.02) for ξ_B. The graph shows that they are related in a non-linear way. One point to consider is that this graph is not symmetric, and parameters have different effects. The interaction between these two parameters shows that these two parameters affect the battle results in the same way. Decreasing any of these parameters will cause Blue to win. Since we can explain η_Z as cyber defensive effectiveness of Red and ξ_B as cyber offensive effectiveness of Red, they affect the battle in the same direction. Also, we can see that η_Z has a higher relative threshold than ξ_B, which gives the same result with the analytical approach.

Finally, we compare the number of recovered Blue (R_B) with number of infected Blue (I_B). This time, unlike the other three comparisons, we compare the number of units

instead of rates. We use a range (0, 200) for both state variables. In this case, the number of Red forces is constant and equal to 1000. The number of Blue forces, however is not constant and changes due to other state variables. Comparing these two factors, we see another non-linear interaction. The interaction between these two state variables comes from the tradeoff between the total size of the Blue fighting force, and the effect of cyber attack on Blue. Noting that initial Red size is constant in all the points in this figure, when infected size gets larger, the total fighting force gets larger, too. This affects the overall battle result in favor of Blue, even if elements of the increased force are infected.

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	0.0005
Red	1000	949	1	50	0.10	0.01	0.0050	0.0005

Table 3. Base parameters for numerical sensitivity analysis figures
Figure 29 is based on this table. The range of parameters are specified on each graph.

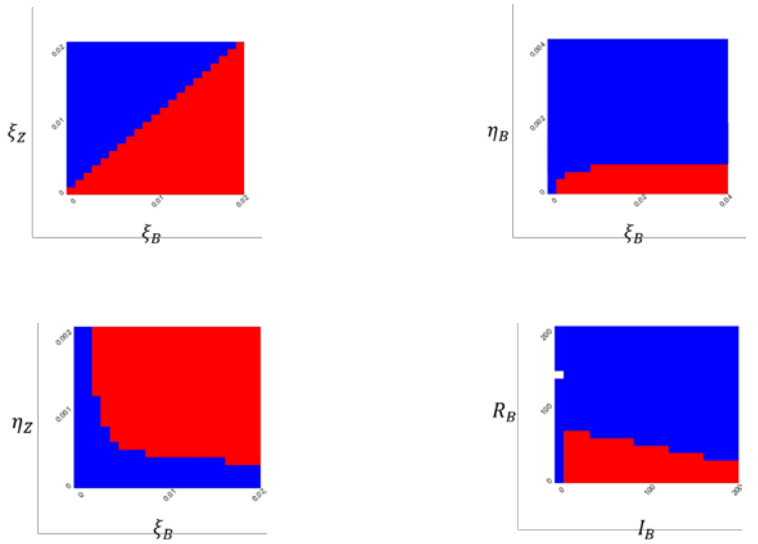

Figure 28. Numerical analysis pairs.
Each graph uses parameters from Table 3. The sensitivity range is specified on each graph.

6. Dynamic State Equations

Starting again with equation (4.11 - 4.18) we follow the steps specified in Appendix D for the following equation:

$$\left(\frac{B}{B_0}\right)^{\xi/\eta} \frac{I_B}{I_0} = \left(\frac{R_B}{R_0}\right)^{\xi/\eta} \frac{S_B}{S_0} \,. \qquad (4.23)$$

This is equivalent to:

$$\boldsymbol{R_B}\left(\frac{\boldsymbol{S_B}}{\boldsymbol{I_B}}\right)^{\boldsymbol{\eta/\xi}} = \boldsymbol{c\,B}, \qquad \boldsymbol{c} = \frac{\boldsymbol{R_0}}{\boldsymbol{B_0}}\left(\frac{\boldsymbol{S_0}}{\boldsymbol{I_0}}\right)^{\boldsymbol{\eta/\xi}} \qquad (4.24)$$

All initial states (S_0, I_0, R_0) belong to *B*. Note that the state variables and parameters should be positive, and *c* is constant.

Equation (4.23) and equation (4.24) are different representations of the model. We keep these equations for different interpretations.

These dynamic state equations provide a solid background to show effects of cyber operations, considering the given spread model. We should keep in mind that *B* is the driver here, and may decrease over time by the kinetic effect. So as the ratio $\frac{B}{B_0}$ drops from an initial value of 1 and approaches 0, all other states are affected by this. Without an attrition effect on *B*, the term $\frac{B}{B_0}$ will be constant (e.g., 1), and the other states will be balanced by these equations. If we know or model the change of ratio $\frac{B}{B_0}$ by an outside model (i.e., kinetic attrition), we can understand the infection level at any time, by given initial conditions.

Equation (4.23) shows a clear picture for changes on *B*. Yet it represents the changes within B explicitly, but depends on other factors such as Z for overall change of *B* (i.e., attrition). If we use the assumption of "no kinetic battle," there will be no attrition,

and $\frac{B}{B_0}$ is 1. Also assume that $\xi = \eta$. In that case, we see the same result with Schramm and Gaver (2013) closed form of *I(t)*, which uses the same assumption.

Equation (4.24) shows that the ratio of *B* to B_0 is inversely related to the ratio of *I* to I_0. Again the ratio of *B* to B_0 is directly related to the ratio of *R* to R_0 and to the ratio of *S* to S_0. These calculations would hold outside of asymptote limits. With this equation we see that, change in the value of *B* affects R_B , attack rates, spread rates and patch rates in different ways.

Equation (4.24) supports a basis for a cost estimation comparison for cyber operation effects. We conclude that the value of *R* affects the overall combat proportional to fraction, whereas the ratio of rates affects the combat exponentially.

7. Cyber Pandemic Threshold

The maximum time of infection is an important breakpoint. We will discuss this issue further in this section. As discussed in Schramm and Gaver (2013) under the assumptions $\beta = \rho = 0,\ \xi = \eta$ the maximum infection time is:

$$\boldsymbol{t_{I_B\,max}} = \frac{\mathbf{1}}{\mathbf{2\xi B_0}} \boldsymbol{ln}[\frac{(\boldsymbol{S_0} + \boldsymbol{I_0})\,\boldsymbol{S_0}}{(\boldsymbol{R_0} + \boldsymbol{I_0})\,\boldsymbol{R_0}}] \qquad (4.25)$$

If we want to estimate time of maximum infected ratio from the start of the battle, we can assume that $I_0 \ll R_0 \ll S_0$, and take I_0 as a small number (e.g., 1). Approximating $\boldsymbol{B_0 = S_0 + R_0}$, that will lead us to:

$$\boldsymbol{t_{I_B\,max}} \cong \frac{\mathbf{1}}{\boldsymbol{\xi}\,(\boldsymbol{S_0} + \boldsymbol{R_0})}\ \boldsymbol{ln}\left[\frac{\boldsymbol{S_0}}{\boldsymbol{R_0}}\right];\quad \boldsymbol{ln}\left[\frac{\boldsymbol{S_0}}{\boldsymbol{R_0}}\right],\ \boldsymbol{I_0} > 0 \qquad (4.26)$$

If we fix the fraction $\frac{\boldsymbol{B_0}}{\boldsymbol{R_0}} = k$, we can summarize the equation as:

$$\mathbf{t_{I_B\,max}} \cong \frac{\mathbf{1}}{\boldsymbol{\xi}\,k\,\boldsymbol{R_0}}\ \mathbf{ln}[k-1];\quad \mathbf{ln}[\mathrm{k}-1] > 1 \qquad (4.27)$$

We can interpret this equation in several ways.

First, from (4.26) we observe that $t_{I_B\,max}$ decreases inversely as rate of infection spread rate ξ increases. That means if ξ is doubled, t will be ½ of the original; and if ξ is increased by 10 times, t will be 1/10 of the original.

The second and less intuitive result from Eq. (4.25) is that R_0 acts the same way. So if the initial recovered size is increased by 10 times, *t* will be 1/10 of the original, also.

Third, the ratio of $\frac{S_0}{R_0}$ is also important; so if it is closer to one, *t* will be closer to zero.

In most cases we can assume to have $R_0 \ll S_0$ and I_0 =1. By this assumption we can see how well maintained (R_0) (regular updates, virus and ID protection, etc.) and poorly maintained units can degrade the response to a cyber attack, thus affecting the combat outcome.

Another way to approach the spread of infection is to find the *pandemic (epidemic) threshold,* which is a lower limit on some attributes of the infection and the cure that indicates how the spread grows throughout the population. The pandemic threshold differs for each epidemic, and is an indicator to foresee when the epidemic grows and when it starts to shrink. Using a differential definition of cyber infection spread to original equation in (4.6), we can summarize the situation in B as :

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \eta_B I_B R_B) > 0 \qquad (4.28)$$

Thus, the threshold is:

$$\xi_B I_B S_B > \eta_B I_B R_B \;\Leftrightarrow\; \xi_B S_B > \eta_B R_B$$

$$\frac{S_B}{R_B} > \frac{\eta_B}{\xi_B} \qquad (4.29)$$

Since S_B and R_B are dynamic in nature, we can interpret that the infection will grow until the ratio of $\frac{S_B}{R_B}$ decreases to the constant $\frac{\eta_B}{\xi_B}$. As was explained previously, when $\xi = \eta$ is assumed, the threshold becomes $S_B > R_B$, and holds with former calculations.

Also, we can interpret that the infected size will increase until some point at time, and then will start to decrease. The time that the sign changes is $\boldsymbol{t_{I_B\,max}}$ and we can come up with an equation as:

$$\frac{\mathrm{S_B}(\boldsymbol{t_{I_B\,max}})}{\mathrm{R_B}(\boldsymbol{t_{I_B\,max}})} = \frac{\eta_\mathrm{B}}{\xi_\mathrm{B}}$$

In most cases the infected side may not know the spread rate of the infection. But as well may estimate the patch rate, number of patched and roughly number of susceptibles. So assuming that infection spread rate is constant, the infection will spread if

$$\xi_\mathrm{B} > \eta_\mathrm{B} \frac{\mathrm{R_B}}{\mathrm{S_B}}. \qquad \textit{(4.30)}$$

In this case, Eq. (4.30) says that $\frac{\mathrm{R_B}}{\mathrm{S_B}}$ acts like a multiplying factor for the patch rate. When $\eta_\mathrm{B} \frac{\mathrm{R_B}}{\mathrm{S_B}}$ is larger than ξ_B, the epidemic starts shrinking. This shows that regardless of the patch rate, if a force keeps a high ratio of recovered units or low ratio of susceptible units (i.e., by constantly updating cyber infrastructure), it would be highly unlikely to spread a disease and cause significant degradation.

8. Cyber Operation Effects on Victory Conditions

We explore cyber epidemic combat models for different objectives, but the main objective is to be able to understand and interpret the effects on battle outcome.

To set the base for victory conditions, we will use the number of survivors in kinetic combat. Thus, the dynamic state equation of kinetic battle can be used to evaluate the number of survivors. So, following the steps from (2.1) and (2.2) we see the closed form equation as $\beta\ (B_0^2 - B^2)\ = \rho\ (Z_0^2 - Z^2)$ by Lanchester (1916). We expect that Blue

wins if $\frac{B_0}{Z_0} > \left(\frac{\rho}{\beta}\right)^{1/2}$, and ends in a draw if $\frac{B_0}{Z_0} = \left(\frac{\rho}{\beta}\right)^{1/2}$ in a battle without cyber effects. We will use the same steps in order to find how cyber operations affect the conditions for victory.

Using B as the number of remaining Blue forces at time t, Z as the number of remaining Red forces at time t, $\overline{\beta}$ as the effective attack rate of Blue at time t, and $\overline{\rho}$ as the effective attack rate of Red at time t, we can estimate victory conditions at time t. Note that this is a dynamic process, and the victorious side can change during the battle time, depending on given parameters. The intention here is not to estimate the winner regarding the initial conditions (which is not possible with these calculations), but is to understand how these parameters affect the battle results. Also, this calculation will reveal whether keeping the current conditions for attack rates at time t for the rest of the battle would lead to victory or not. Blue wins the battle as long as

$$\frac{\boldsymbol{B}}{\boldsymbol{Z}} > \left(\frac{\overline{\boldsymbol{\rho}}}{\overline{\boldsymbol{\beta}}}\right)^{\mathbf{1/2}} \qquad \textit{(4.31)}$$

Another important question is how long one side must keep cyber superiority in order to win. We will look for a sample situation where Blue is defeated. Then we will increase the Blue's defensive cyber operation effectiveness (η_B) to see if Blue is victorious.

Following figures represent a sample comparison for two sides, with Blue exposed to cyber operations. Initial force ratio is 1, so victory of forces depends solely on attack rates. The shaded area is when Blue wins, (respectively, the white area is when Red wins), if we were to keep Blue's attrition rate at a value in the shaded area (respectively the white area) for the remainder of the combat.

In the controlled numerical experiment, we keep every condition the same and set η_B= 0.0002 for Figure 29, and set η_B= 0.0003 for Figure 30. Surprisingly, even this small change can lead to the turnover of the victory in the battle. Various graphs can be produced by trial, but this single experiment tells enough for the importance of cyber operations.

Figure 29 summarizes the attack rates for a kinetic battle which Red wins. We see that Red wins the kinetic battle when the infected units were high in ratio in Blue, because its attacking power was affected significantly. We can conclude that if Red is able to prevent Blue from recovering or if Blue did not invest in cleaning the infection, the battle would result differently.

Figure 30 summarizes the attack rates for the same battle (same parameters) when Blue was able to increase its cyber infection patch rate by 50% and win the kinetic battle.

Shaded regions are the conditions (at time t) where Blue is victorious at the end of the battle, and white regions are for Red.

These discussions are intended to answer some questions about the effects of time of shock, time of recovery, and the size of the forces at these times. We explored what can affect victory conditions, but the methods used in this chapter represent just one way to uncover these questions, and there are various other ways to do it. We have assumptions regarding to epidemic model and combat model which affects the course of discussions. Specific scenarios used for numerical experiments explain proposed models in these specific conditions. There are various ways to change and extend the topics discussed in this section, and we will give some examples in next chapter for several different model types that can be explored in similar ways.

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	***0.0002***
Red	1000	949	1	50	0.045	0.045	0.0050	0.0005

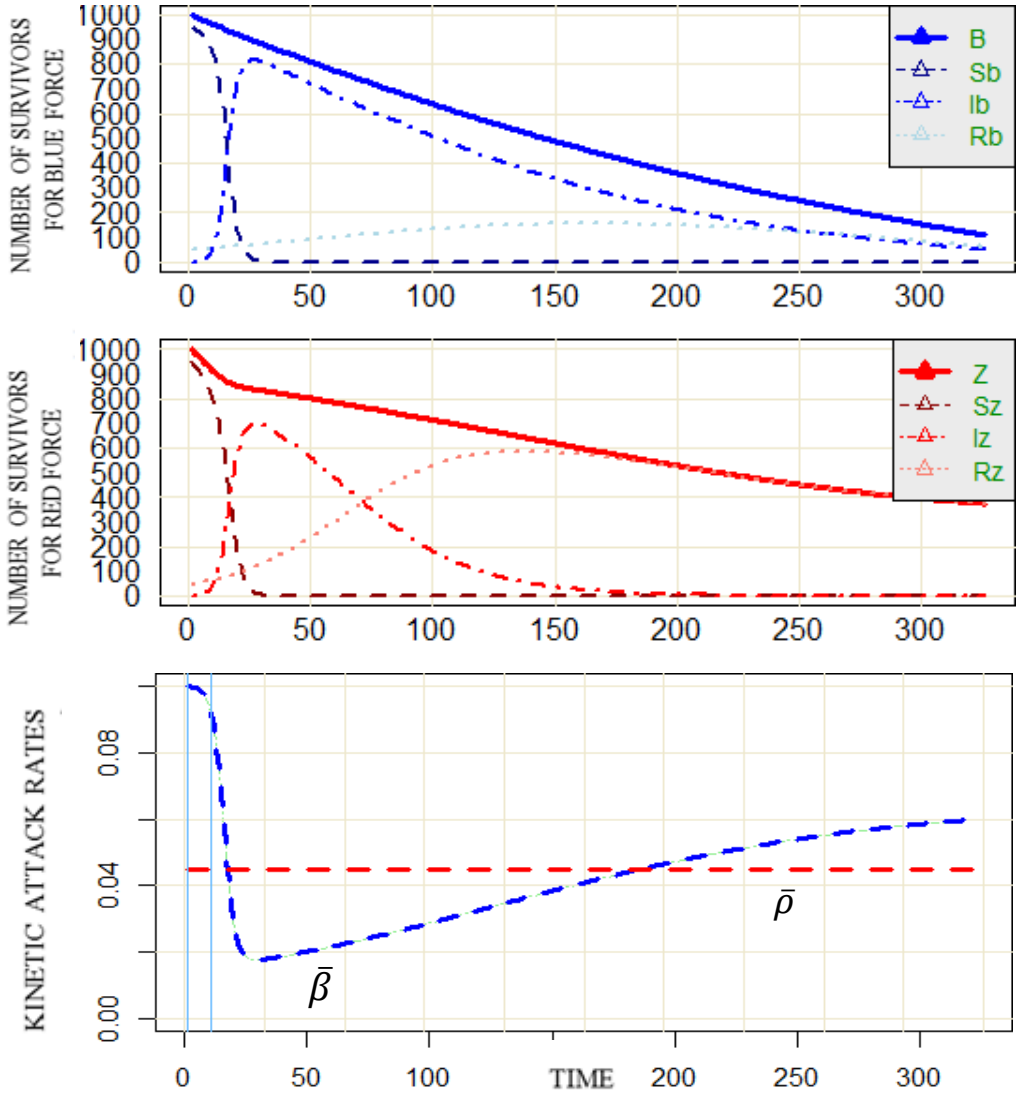

Figure 29. Change of attack rates
(Time is multiplied by 10.) (η_B**= 0.0002).**

Parameters								
	Initial number of the Force (B, Z)	Initial number of Susceptibles (S_B, S_Z)	Initial number of Infected (I_B, I_Z)	Initial number of Recovered (R_B, R_Z)	Attrition rate normal (ρ_U, β_U)	Attrition rate degraded (ρ_D, β_D)	Infection spread rate (ξ_B, ξ_Z)	Infection patch rate (η_B, η_Z)
Blue	1000	949	1	50	0.10	0.01	0.0050	***0.0003***
Red	1000	949	1	50	0.045	0.045	0.0050	0.0005

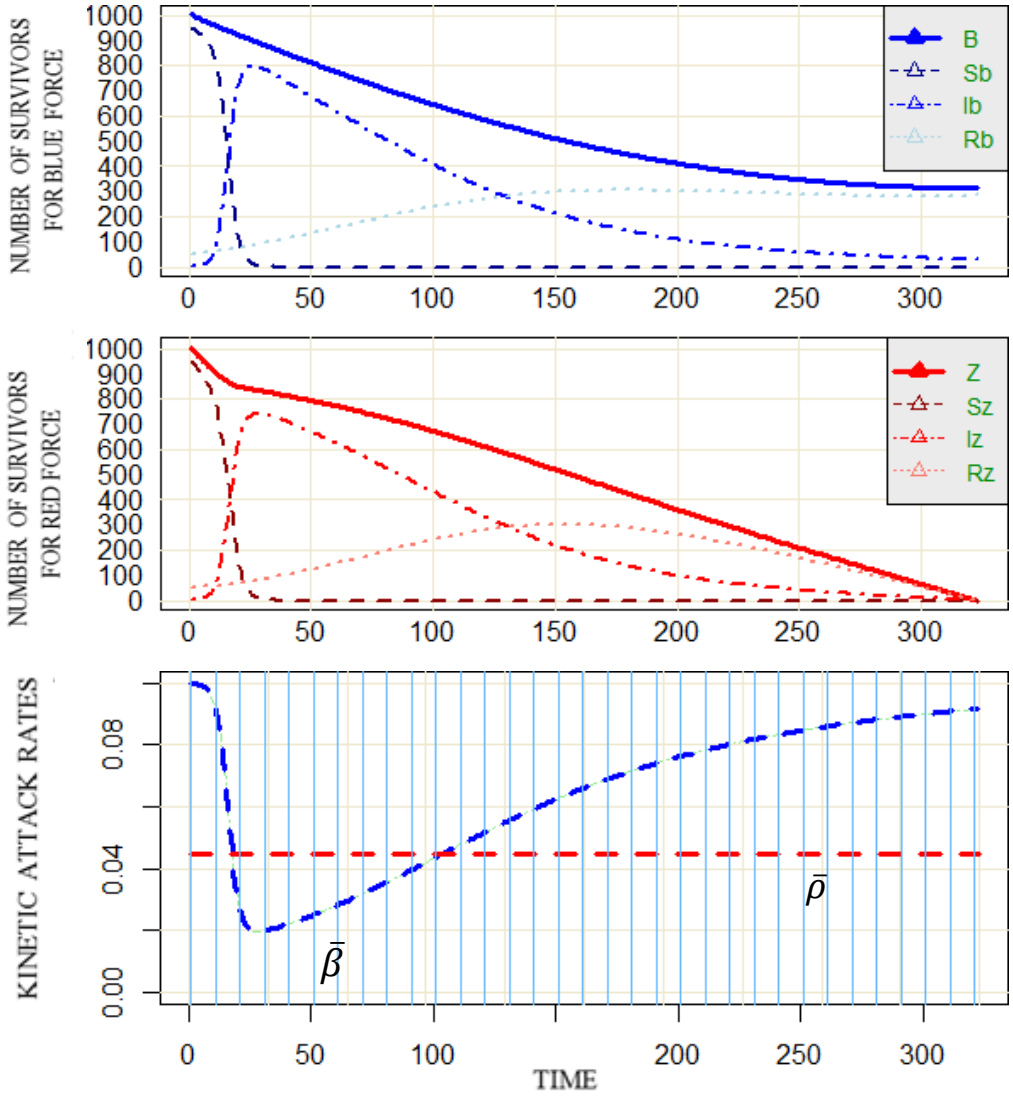

Figure 30. Change of attack rates with 50% increased effective infection patch rate for Blue (Time is multiplied by 10.) ($\boldsymbol{\eta_B = 0.0003}$).

V. PROPOSED EXTENSIONS TO DISCUSSED MODELS

In Chapter IV, we explored some of the attributes of the basic cyber epidemic combat model. In this chapter, we consider different attributes of a cyber attack process and try to expand the model along with these considerations. In order to combine the kinetic battle with cyber operations, the model discussed in Chapter IV needs to be adjusted time-wise. This is because events can happen faster in cyberspace as compared to kinetic space (Andress and Winterfeld 2013). In other words, we differentiate *cyber time* with *kinetic battle time*. We use *scaled-cyber time* in the study first to introduce new aspects with normalized values, and *non-scaled cyber time* after that for time considerations. These models propose only a way to represent a certain attribute, and there are several more ways to model these attributes, and also there are several more attributes.

As discussed in Schramm and Gaver (2013) and explained in Andress and Winterfeld (2013) time-scale can be an issue when combining kinetic attacks and cyber attacks. We categorize the extensions into two main parts; as scaled time discussions, and non-scaled time discussions. Time scale especially affects dynamic calculations, which were discussed in Chapter IV. The calculations for cyber infection spread may be even unnecessary because of the different time scales with cyber battle and kinetic battle. If the cyber infection time is not in sync (or not scaled) with kinetic battle time, this will cause two possible outcomes: either the kinetic battle outcome is dominated by infection regardless of changes in rates and numbers, or it is not affected at all. In contrast, if the kinetic battle time is scaled to cyber time, the battle will be affected anyway, but the effect will be dependent on some factors, such as infection spread rates, number of infected units, etc.

Although we proposed various extensions to the basic model in this chapter, such as adding different intrusion times, defense capabilities or adding a second type of infection to the system, due to time constraints in this study we leave it to the reader to obtain numerical results. Saying that these are some proposed models, intended to explain some different aspects of cyber operations, these extensions need to be analyzed both analytically and numerically in detail.

A. SCALED CYBER TIME – KINETIC COMBAT TIME

In this part, we explore different extensions to the base model, constructed in Chapter IV. We introduce different coefficients and modifications to the model depending on attack/ defense type. We introduce one expression for each model on top of the base model. These extensions work properly if all states are positive. For purposes of exposition, we suppress time-dependence notation, e.g., $S_B = S_B(t)$. **Note that these figures show only positive values. Signs can be determined by the direction of flow.**

1. The Base Case

As a reminder to the reader, here we summarize the model and parameters in the base case scenario from Chapter IV. We then extend the base case scenario by introducing new terms to represent different scenarios of interest.

B : level of Blue force at time t
Z : level of Red force at time t
ξ_B : Infection spread rate within B
η_B : Infection patch rate within B
ξ_Z : Infection spread rate within Z
η_Z : Infection patch rate within Z
ρ_U, ρ_D : Normal attack rate, and decreased (by infection) attack rate of Z on B
β_U, β_D : Normal attack rate, and decreased (by infection) attack rate of B on Z

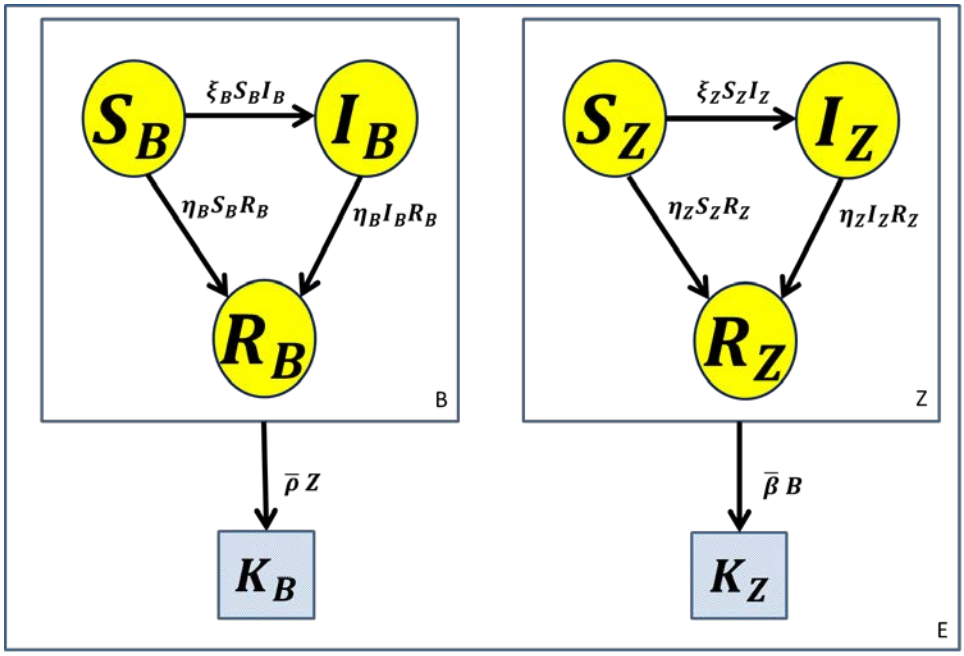

Figure 31. A two-sided Cyber epidemic combat model.

2. Intrusion Rate

In Chapter IV, we explored the importance of the first infection on the overall system dynamics and battle outcome. We now introduce a new term to represent this initial infection. Specifically, we define the following.

θ_B : Infection start (intrusion) rate within B
θ_Z : Infection start (intrusion) rate within Z

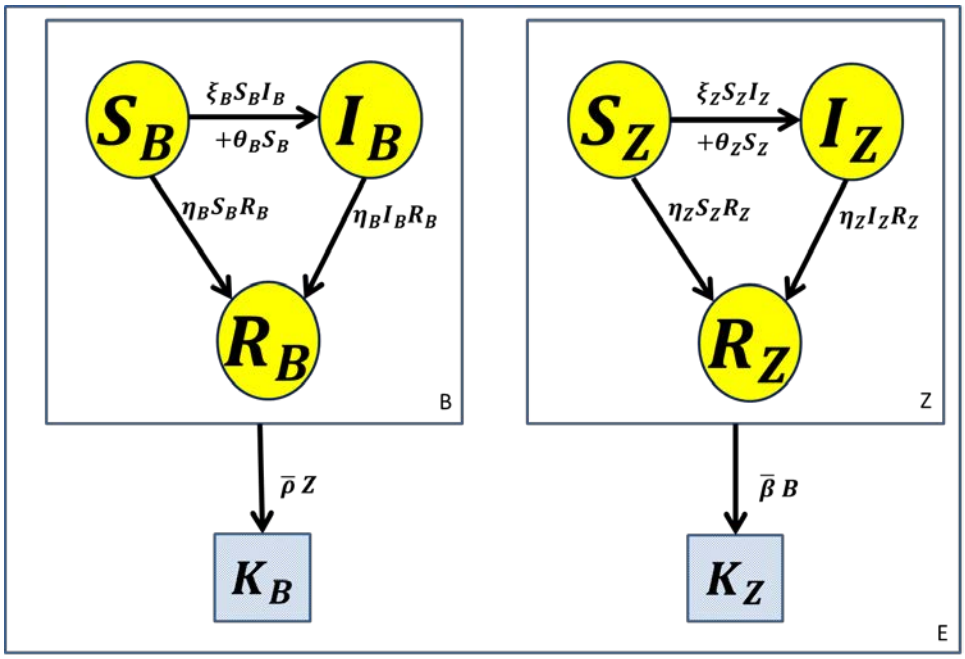

Figure 32. A two-sided Cyber epidemic combat model with intrusion rates.

The new term θ_B represents the intrusion rate to Blue in order to start an infection. This is a crucial term to estimate effectiveness of defensive actions of B and can be estimated from real data on cyber penetration tests on combat units.

The Blue Forces is infiltrated and infected at the rate of θ_B in a given timeframe. Since penetration is the toughest part of a cyber attack, this rate is different from the spread rate and in general should be much smaller.

We formulate the dynamics for the one-sided model only to simplify this process; the other side will be symmetric.

$$\frac{dB}{dt} = -\bar{\rho}\, Z \qquad (5.1)$$

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B - \theta_B S_B - \eta_B S_B R_B) + \frac{dB}{dt}\frac{S_B}{B} \qquad (5.2)$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B + \theta_B S_B - \eta_B I_B R_B) + \frac{dB}{dt}\frac{I_B}{B} \qquad (5.3)$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B) + \frac{dB}{dt}\frac{R_B}{B} \qquad (5.4)$$

We may use intrusion rate in our model for a more realistic approach. In real world, unlike in our model in chapter IV, the first infected unit can be found and patched before spreading the infection in the adversary, which would affect the course of the battle. On the other hand, there would be multiple intrusions in a cyber attack to make sure the infection spreads. We may represent these two actions with θ_B.

Second, representing the intrusion rate separately will allow us to assess how it affects a cyber attack. Note that there are special designed simulations to represent cyber intrusion to systems. So, gathering data and comparing the model with the data is an area of interest, which is very applicable.

3. Defense Rate

A cyber defensive action can be modeled in different ways, depending on the nature of the cyber operation. The main subdivisions can be passive defense and active defense. We propose two different approaches for these two types of defensive actions.

a. Constant Defense Rate

In the context of a mixed-epidemic model, passive defense means that B can reduce the spread of an infection at a constant rate using passive defensive actions, i.e., firewall, automated virus protection programs, automated network transfer reductions, etc. These actions generally use automated procedures with dedicated resources or out-sourcing. We assume these actions do not affect the kinetic attack rate, are not related to the number of fighting units, and are reducing the spread as a constant rate alone, if that is positive. To reflect this dynamic in our system equations, we introduce the following terms.

γ_B *: Threat detection rate of B*
γ_Z *: Threat detection rate of Z*

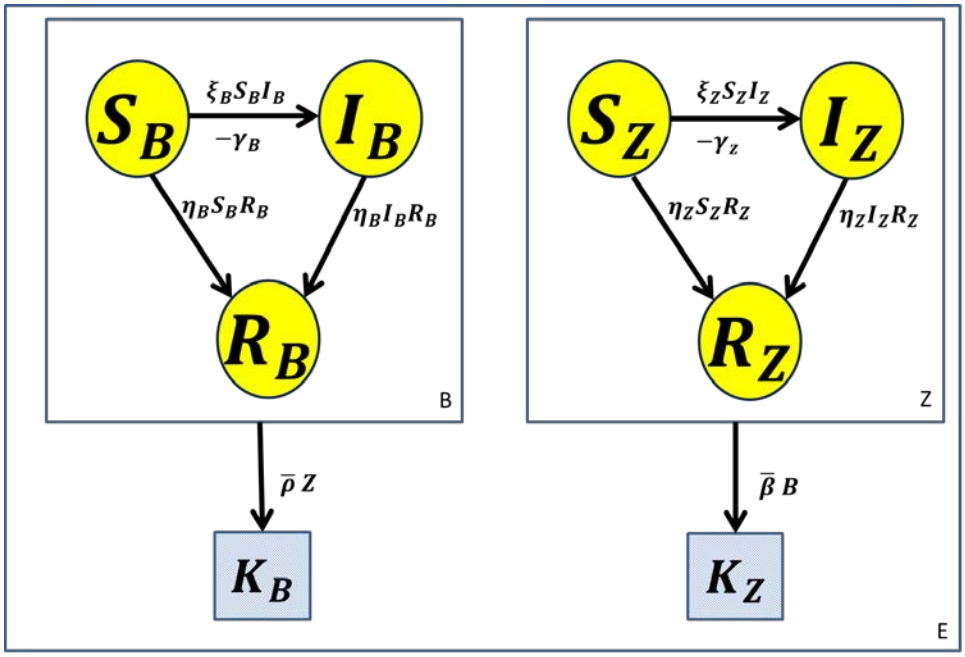

Figure 33. A two-sided Cyber epidemic combat model with constant defensive action.

Again, we formulate one-side to simplify the exposition, with the other side symmetric.

$$\frac{dB}{dt} = -\bar{\rho}\, Z \tag{5.5}$$

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B + \gamma_B - \eta_B S_B R_B) + \frac{dB}{dt}\frac{S_B}{B} \tag{5.6}$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \gamma_B - \eta_B I_B R_B) + \frac{dB}{dt}\frac{I_B}{B} \tag{5.7}$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B) + \frac{dB}{dt}\frac{R_B}{B} \tag{5.8}$$

Note that the intention here is adding the model the effects of automated processes for cyber systems. These processes require a certain amount of resource, which will be used to reduce the spread of infection. Also, if the infection spread is not fast enough and if it does not consume all of these automated resources, these will be used to clean the infected units. Cleaning the infection by an automated process is not patching the unit, but is taking away the degrading effect, so that these units are susceptibles and can be infected again, until patched by an *R*. This model works if $S_B, I_B, R_B > 0$.

b. Active Defense Rate

In contrast to passive defense, active defensive actions generally use some resources related to the fighting force, and the use of these resources detracts from the kinetic capability of the force. To be more specific, active defense of Blue constricts use of cyber-related parts (i.e., communication devices, navigation devices, headquarter computers) in order to reduce the spread of infection in Blue, which slows down the cyber infection spread as well as slowing down the patch updates in Blue. However, this measure reduces the kinetic attack rate of Blue also, because the cyber defender (Blue) restriction of use of cyber-related parts may as well reduce fighting capability of cyber defender as well as reducing spread of cyber infection.

T_B *: Information process rate of B* $(0 \leq T_B \leq 1)$

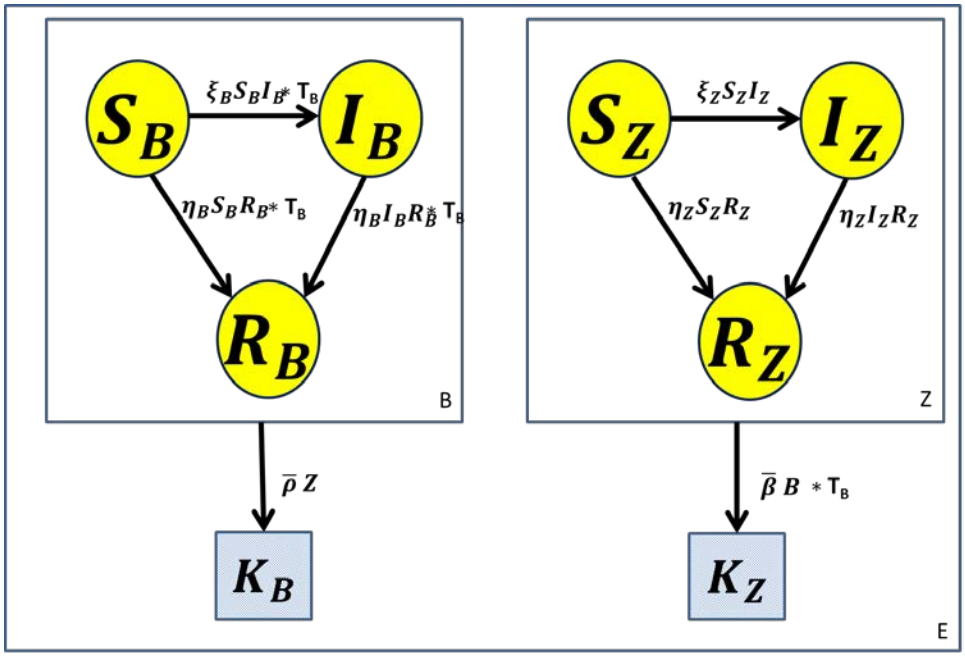

Figure 34. A two-sided Cyber epidemic combat model with dynamic defensive action.

$$\frac{dB}{dt} = -\bar{\rho}\, Z, \qquad \frac{dZ}{dt} = -\bar{\beta}\, B\, T_B \tag{5.9}$$

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B - \eta_B S_B R_B)\, T_B + \frac{dB}{dt}\frac{S_B}{B} \tag{5.10}$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \eta_B I_B R_B)\, T_B + \frac{dB}{dt}\frac{I_B}{B} \tag{5.11}$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B)\, T_B + \frac{dB}{dt}\frac{R_B}{B} \tag{5.12}$$

$$\frac{dS_Z}{dt} = (-\xi_Z S_Z I_Z - \eta_Z S_Z R_Z) + \frac{dZ}{dt}\frac{S_Z}{Z} \tag{5.13}$$

$$\frac{dI_Z}{dt} = (+\xi_Z I_Z\, S_Z - \eta_Z I_Z\, R_Z) + \frac{dZ}{dt}\frac{I_Z}{Z} \tag{5.14}$$

$$\frac{dR_Z}{dt} = (+\eta_Z R_Z S_Z + \eta_Z R_Z I_Z) + \frac{dZ}{dt}\frac{R_Z}{Z} \tag{5.15}$$

The variable defense rate of Blue (T_B) models the information process rate in case of a cyber attack. If the infection spread is high, reducing the process rate to 0 will stop the spread of the infection, and the cure of the infection, and can be considered at max protection from a cyber attack level with a trade-off on reducing communication, and decreasing the kinetic attack rate to 0. Keeping the rate at 1 will not have any effect on cyber attack and can be considered as weakest cyber protection, but the kinetic attack will not be affected by reduced information process, also.

4. Intelligence Level of Cyber Attacker

We are interested in the situation where an attacker (Red) has an intelligence level of which members of Blue are in state R in defender (Blue). So, the attacker wants to aim for just for those Blues that are in state R instead of overall Blue forces, to not to kill infected units and susceptibles. We introduce a new expression (μ_B) to model this situation.

The expression μ_B represents the level of intelligence distinguishing R_B. So, if μ_B is set to 0, it means that the attacker has no specific information about R_B and aims at Blue as a whole as in the basic model. If μ_B is set to 1, it means that the attacker has perfect information about R_B and aims only at R_B, and causes no attrition on S_B or I_B. Any intelligence level between 0 and 1 can be used in the model.

We will formulate one side to simplify this process, and the other side will be symmetric.

$\boldsymbol{\mu_B}$: Attacker's intelligence level on state R_B ($0 \leq \boldsymbol{\mu_B} \leq 1$)

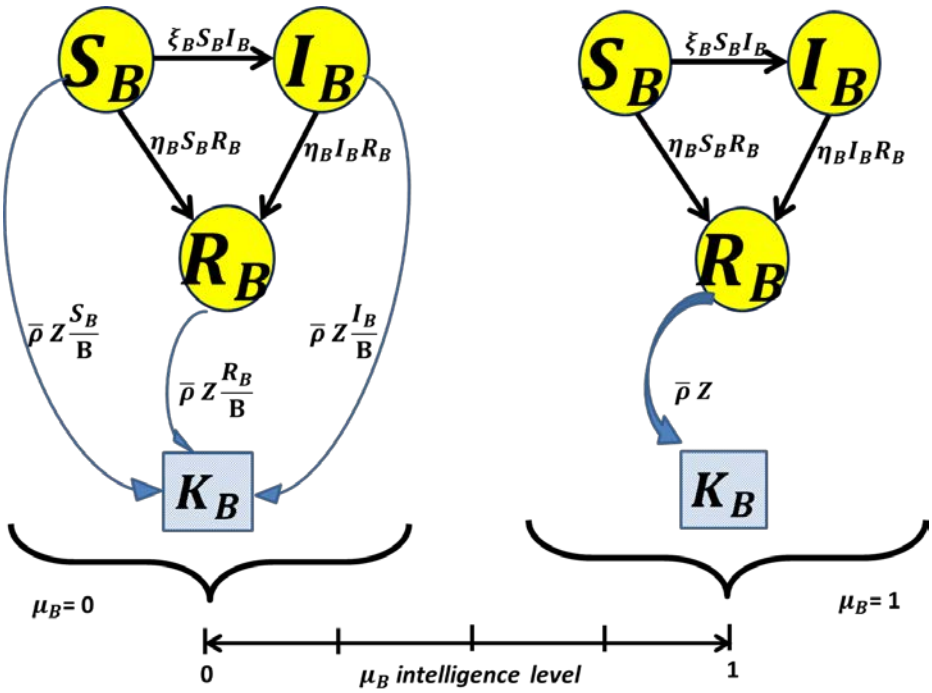

Figure 35. A notional figure about using intelligence level. Change in one side (Blue) by intelligence level is represented

$$\frac{dB}{dt} = -\bar{\rho}\, Z \qquad (5.16)$$

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B - \eta_B S_B R_B) + \frac{dB}{dt}(1-\mu_B)\frac{S_B}{B} \qquad (5.17)$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \eta_B I_B R_B) + \frac{dB}{dt}(1-\mu_B)\frac{I_B}{B} \qquad (5.18)$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B) + \frac{dB}{dt}((1-\mu_B)\frac{R_B}{B} + \mu_B) \qquad (5.19)$$

This model can be used to represent a phase, if the cyber attacker wants to spread the infection, and the intention is to first clear the recovered units, and then focus on to susceptible units and infected units. This may be the case when the adversary has a limited size of recovered units, which can be completely killed in a short time.

Another use area may be the one if the cyber attack is very effective about reducing the kinetic capability of the adversary, and can spread fast enough, but the kinetic attack costs (or risks) are high.

The common point in these two cases is the aim to spread the infection, whether to collect intelligence, or to reduce kinetic attack capability of the adversary.

5. Use of White Population for DDoS Attack

This is a model for Distributed Denial of Service (DDoS) attack, which uses infection spread in another network. A DDoS attack is an indirect attack type, which intends to decrease the usable capacity of communication networks by sending constant messages and by generating a heavy burden of unnecessary message traffic. So, DDoS networks (or botnets) attack a given target with brutal cyber force as a physical attack and reduce the capacity to communicate.

We simplified the B states to Working (W_B) and Disabled (D_B). $D_B + W_B = B$ We assume Disabled B cannot communicate any other units; thus, it is ineffective. So, $\beta_D = 0$ in this case. We will use β_U as $\bar{\beta}$.

W Population : Cyber attack capability (Being used unintentionally)
W_B *: Working units in B*
D_B *: Disabled units in B*

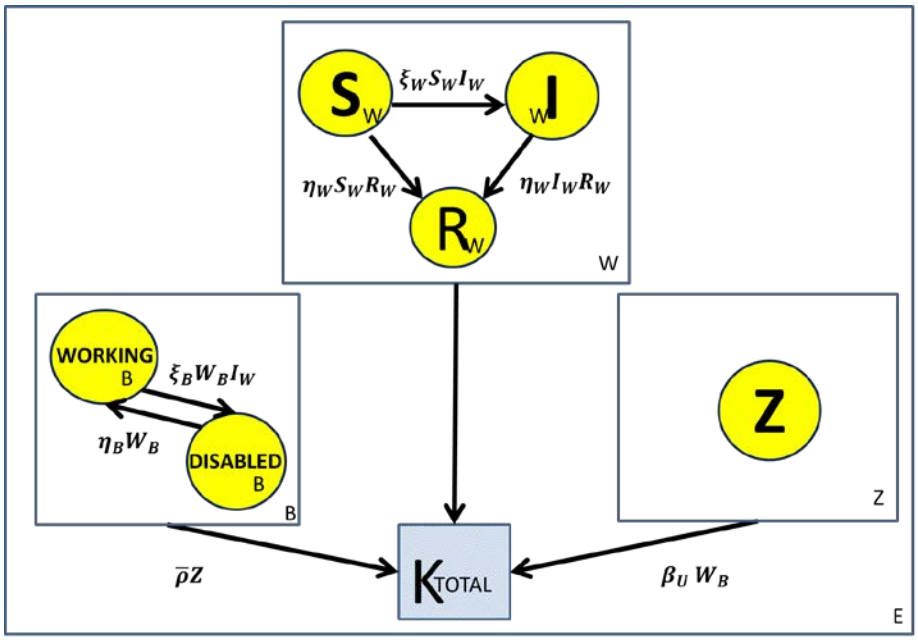

Figure 36. A Cyber epidemic combat model with DDoS attack.

$$\frac{dB}{dt} = -\bar{\rho}\, Z \tag{5.20}$$

$$\frac{dZ}{dt} = -\beta_U(W_B) \tag{5.21}$$

$$\frac{dW_B}{dt} = (-\xi_B W_B I_W + \eta_B W_B) + \frac{dB}{dt}\frac{W_B}{B} \tag{5.22}$$

$$\frac{dD_B}{dt} = (+\xi_B W_B I_W - \eta_B W_B) + \frac{dB}{dt}\frac{D_B}{B} \tag{5.23}$$

$$\frac{dS_W}{dt} = (-\xi_W S_W I_W - \eta_W S_W R_W) \tag{5.24}$$

$$\frac{dI_W}{dt} = (+\xi_W I_W S_W - \eta_W I_W R_W) \tag{5.25}$$

$$\frac{dR_W}{dt} = (+\eta_W R_W S_W + \eta_W R_W I_W) \tag{5.26}$$

Use of white population is the cheapest and the most common way conduct a cyber attack. Also, there are a few recent incidents in real world that shows these types of attacks can be used with a kinetic attack (before or after a kinetic battle starts). Modeling this phenomenon is an area of interest, and the models that discussed in Chapter IV can be modified in various ways for further research. We propose one way, to open this path for the discussions, but adding different attributes and modeling different phases may be necessary along with using these models on real world data.

6. Smart Cyber Ammunition Attack

This section introduces a smart cyber ammunition attack model. Unlike previous models, a *smart cyber ammunition* attack can be used to kinetically damage a cyber-aimed target. In this model, Red does not have cyber capability, and Blue conducts a smart cyber ammunition attack by using two different types of infections on Red. Consider these two infections as the moving parts of a cyber weapon, which only works together. So, they spread in stealth and do not affect the infected unit's kinetic capability. In this case for Red, a unit is disabled permanently (detonated) with a rate, which is the *detonation rate* referred as δ, when two infections (I_1 and I_2) collide on the same unit at the same time. So, if a unit is infected with one of these infections, then two options appear: it would be cured for good, or it will have the other infection and detonate with a rate. These infections do not have any effects otherwise, and a patch for one infection does not limit the other infection.

To create a smart cyber ammunition, using two different types of infections may be essential, because a supply chain attack would be conducted. It means that if the cyber attacker (Blue here) uses one type of infection, every time infected part is used in a machine (aimed or not), it will be detonated with a rate, which may cause unwanted damage. However, using two types of infections for two different parts would limit the risk to cause an unwanted damage to a very low level (maybe insignificant). In other words, Blue may not be able to find a part used in just (aimed) Red units, but may be able to find two parts that can just be used on aimed units together, and detonate aimed Red units with a cyber attack using two infections that spread on these two parts .

Since this is a stealth weapon, a lower detonation rate helps to hide the infected parts. In other words, if we set δ to .99, each time these two parts used together, there is a .99 chance to cause a cyber attack. However, this may not be desirable if the intention is to confuse the users of these parts. It would be an obvious evidence if the cyber weapon activates each time these two parts are used together, so we want to randomize that process and choose a probability to activate these infections depending on the tactical

approach. If Blue keeps the detonation rate low, it will cause Red to use less resources about cyber protection (e.g., $\eta_1, \eta_2 \cong 0$) and will help to spread these infections easier.

δ : Infection detonate rate ($0 \leq \delta \leq 1$)

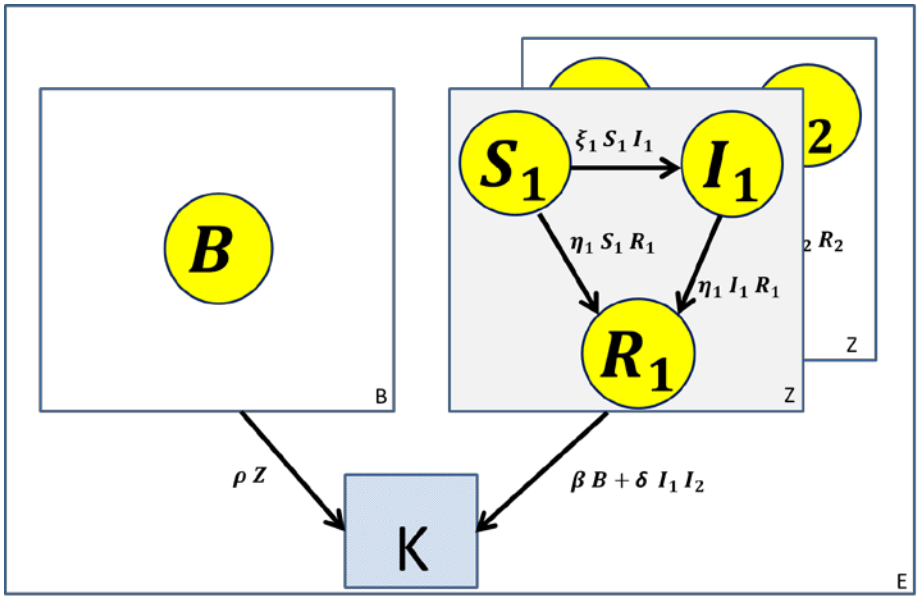

Figure 37. A smart cyber ammunition model .

$$\frac{dI_{detonate}}{dt} = -\delta\, I_1\, I_2 \qquad (5.27)$$

$$\frac{dB}{dt} = -\rho\, Z \qquad (5.28)$$

$$\frac{dZ_{kinetic}}{dt} = -\beta\, B \qquad (5.29)$$

$$\frac{dS_1}{dt} = (-\xi_1 S_1 I_1 - \eta_1 S_1 R_1) + \frac{dZ_{kinetic}}{dt}\frac{S_1}{Z} \qquad (5.30)$$

$$\frac{dI_1}{dt} = (+\xi_1 I_1 S_1 - \eta_1 I_1 R_1) + \frac{dZ_{kinetic}}{dt}\frac{I_1}{Z} + \frac{dI_{detonate}}{dt} \qquad (5.31)$$

$$\frac{dR_1}{dt} = (+\eta_1 R_1 S_1 + \eta_1 R_1 I_1) + \frac{dZ_{kinetic}}{dt}\frac{R_1}{Z} \qquad (5.32)$$

$$\frac{dS_2}{dt} = (-\xi_2 S_2 I_2 - \eta_2 S_2 R_2) + \frac{dZ_{kinetic}}{dt}\frac{S_2}{Z} \qquad (5.33)$$

$$\frac{dI_2}{dt} = (+\xi_2 I_2\, S_2 - \eta_2 I_2\, R_2) + \frac{dZ_{kinetic}}{dt}\frac{I_2}{Z} + \frac{dI_{detonate}}{dt} \qquad (5.34)$$

$$\frac{dR_2}{dt} = (+\eta_2 R_2 S_2 + \eta_2 R_2 I_2) + \frac{dZ_{kinetic}}{dt}\frac{R_2}{Z} \qquad (5.35)$$

We see a new concept in cyber attack in this case. The cyber attacker causes kinetic damage on the adversary with only using cyber force. Since there are some incidents like this in real world, this concept is in an area of interest. The proposed model, however, is just a glimpse on the topic, which has a variety of aspects and ways to model, and needs detailed discussions.

B. TIMELINE LIMITATIONS FOR PARAMETERS

In Figure 38, we summarize a cyber attack process on a timeline. Each parameter models different types of effects on different phases of the process. Red labels are the attack phases for the cyber attacker, and blue labels are the defensive phases for the cyber defender. These phases are discussed in Appendix B in detail. *Peace* represents the period before and after a cyber attack, the phase without cyber considerations. *Access* represents the action of infiltration to the system, by injecting the first infection (I=1). The time between these two phases is considered as t_1, which includes reconnaissance, gathering information and conducting intrusion techniques. *Escalation* represents the period after the intrusion, until the Assault. This phase is considered as $t_2 + t_3$. *Assault* represents the action when cyber attack affects kinetic world, which may be a process (from t_1 to the end of the battle) or a shock (when the infected ratio is at a desired level). Escalation phase is considered in two parts as from the side of defender. t_2 which is the period until the cyber defender detects the vulnerability, and t_3 which is the period until the defender publishes a patch. Then the recovered units start to work until the cyber battle is over, which is the period represented as t_4. The introduced terms are represented in the timeline, to be more specific about where we can start using these parameters within a cyber attack scheme.

The time phases are explicitly mentioned because although the model in Chapter IV covers t_4, a cyber attack needs a larger period of time. The proposed extensions are one way to represent and explore these phases,

Now consider that we have some limited resource, and we allocate this to decrease some of these phases. So, “How does increasing intrusion time affect the cyber attack?” or “What is the effect of detecting vulnerability earlier?” are questions of interest, but we limit the scope of this study to t_4 and the effects of Assault considering infection effectiveness and defense effectiveness.

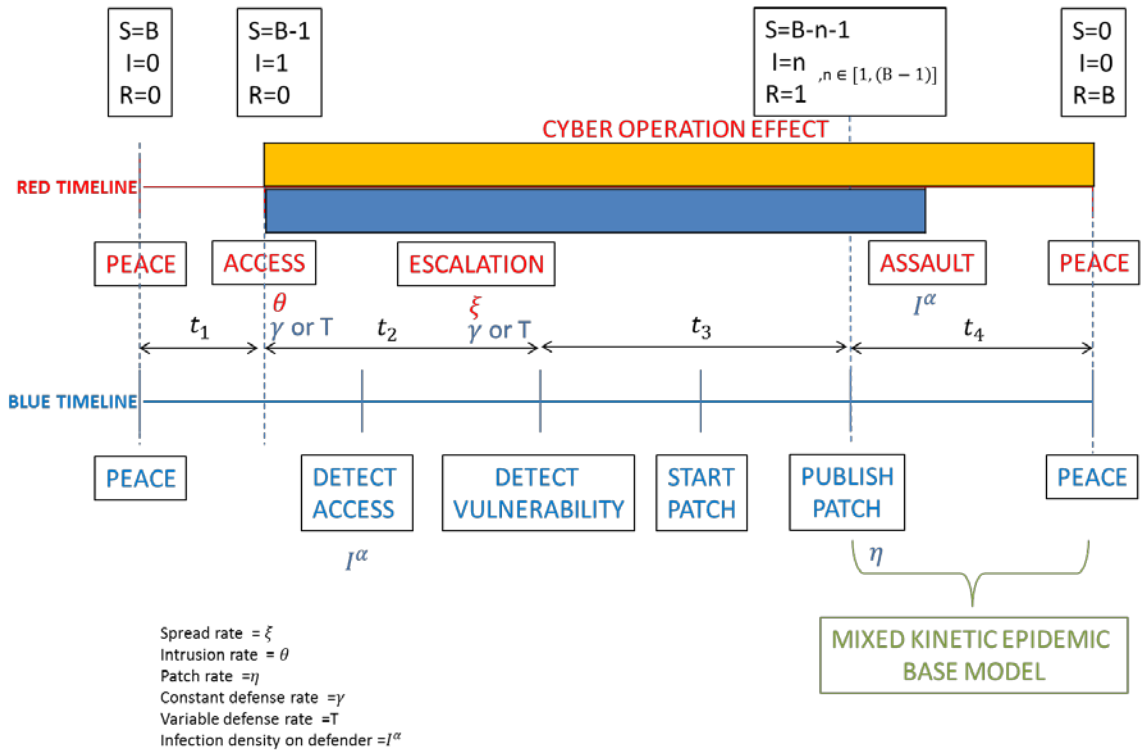

Figure 38. The range of parameters in a cyber attack.

C. NON-SCALED CYBER TIME – KINETIC COMBAT TIME

In this part, we will explore two types of cyber situations which cause instant effects on kinetic battle. For these two cases, we do not need to go into detail and estimate infection spread rates or numbers. The reason is that the outcome for kinetic battle would be the same, and regardless of spread, we can assume that the attack rate drops down from β_U to β_D instantly, after a certain point.

The first case is about the effects of infection spread and patch rates, which may cause to dominate cyber battle or kinetic battle The second case is about the effect of a high value target, which may change the kinetic attack rate of the force only by itself if infected.

1. High Spread Rates and Patch Rates

We will use the time scale from Schramm and Gaver (2013) as a reference point to separate the cases in which cyber effects such as spread rates (i.e., ξ) are too fast and affect the kinetic battle instantaneously. In the same manner, cyber effects can be too small and ineffective if the patch rates (i.e., η) are too fast. There are two possible outcomes:

First case is when the condition discussed in Schramm and Gaver (2013) holds:

$$S_0^2\, \xi_B\, (\beta_U - \beta_D) \gg 4\, \beta_U\, Z_0^2\, \bar{\rho}\,. \tag{5.36}$$

This means too fast cyber time for the kinetic battle. So, in case of a shock, cyber operation result is effective by t_* on kinetic battle. The result of this attack depends on one condition. The condition is:

$$\eta_B \ll \xi_B\,.$$

That means the infection has too high spread rate, and at time t_* attack rate will change to β_D This causes a shock effect as described in Chapter III.

Or the other way, the condition does not hold,

$$\eta_B \gg \xi_B\,.$$

Meaning that the patch rates are too high for the infection to spread (or survive), so at time t_* attack rate does not change from β_U, and the cyber attack has no effect on kinetic battle.

Second case is when the discussed condition (5.36) does not hold:

$$S_0^2\, \xi_B\, (\beta_U - \beta_D) \ll 4\, \beta_U\, Z_0^2\, \bar{\rho}\,.$$

This means too slow cyber time for the kinetic battle. In other words, kinetic battle will be ended, long before cyber attack has an effect on the battle. So, in this case cyber operation result is not effective on kinetic battle.

2. Single Critical Cyber Target

The second case which may cause an instant effect is when the force under cyber attack (Blue) has a crucial target that gathers and controls most of the cyber movements, which creates a natural bottleneck for cyber infrastructure. In this case, the spread in other units can be ineffective, but infection of these bottlenecks can affect a whole network. Although these devices are secured with more protection layers than ordinary units, the protection level never goes to 100%, and infection of these units may even be disastrous for defenders. In these cases, headquarters main command and control devices, main communication servers, fire control and flight sync units, etc., can be possible targets.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY AND RECOMMENDATIONS

We provide an overall summary of the thesis, followed by some insights derived in this study, including recommendations, which may help to support decision makers in an analytic approach. Future research combines some topics in a sequence that will help to improve and validate the results of this study, and extend the range of use.

A. SUMMARY

In cases involving cyber incidents there is an unexpected impact, both in business and the military. The importance of cyber operations and cyber defensive measures are not just some buzzwords, as recently evidenced by the U.S. establishment of its first official "Cyber Force," and stated cyberspace as a main domain for military operations along with land, air, sea and space.

This thesis is motivated by the need to understand analytically the effects of cyber warfare on real battles. We extend two recently published models that use Lanchester equations as a primary model for combat. Our extension of the model by Schramm (2012), *Lanchester with discontinuities*, can be used to model physical attacks, supply chain attacks or DDoS attacks, all of which can have discontinuous impacts on combat. The second model of Schramm and Gaver (2013), *the mixed epidemic combat model*, can be used to represent viral and malware attacks, along with special designed cyber tools. The impacts of these attack concepts can be gradual or continuous, but can turn into a shock effect with some tactical arrangements such as event or time triggers.

Our objective is to answer questions about the impact of cyber operations on kinetic battle. Exploring some analytical and numerical results in this pursuit, we consider tradeoffs between the model parameters to answer questions like "what is the value of a cyber unit?," "how much time does the defender have, to recover to not to lose?," or "if one side faces a larger force, what are the cyber requirements to overcome that advantage." Various special cases depict the effects of battlefield capabilities, kinetic and

cyber. Cyber capability can potentially diminish the attack power of an opponent for an arbitrary but decisive time.

B. RECOMMENDATIONS

The results from the shock cyber model suggest the following measures to reduce the expected loss value due to a cyber attack.

First, use distributed networks, each in control of a limited number of units, or use cloud networking, if applicable. As the force size which is susceptible to an infection gets larger, the loss from the cyber attack will get larger. So the cyber effects use similar mechanics as with Lanchester square law force concentration rule. But unlike conventional kinetic battles, for a cyber attacker it is easier to cause damage to, and defeat a larger force compared to defeating two smaller forces.

Secondly, defensively delay the opponent cyber attack as much as possible. If the cyber attack shock can be delayed from time t to time 2t, the effect of the cyber attack reduces to ~ ¼ of the cyber effect at time t.

Thirdly, defensively shorten the recovery time from a cyber attack, because the duration of the cyber attack increases the effects of that attack. If the duration of the cyber effect at time t halves, the damage by cyber attack can be reduced to ¼ of that at time t.

The damage caused by the cyber attack depends on its effectiveness: reduction of adversarial kinetic capability. The effectiveness of the attack can be reduced by increasing the resilience of cyber systems, such as by having trusted system backup points, rehearsing system resetting to a backup point, suitably frequent scans for probable intrusions, along with logging and inspecting network traffic. If the attack is not very effective, the defender may even choose not to allocate any resources to recover from it.

Results from the continuous cyber effects model suggest the following measures to mitigate a cyber attack.

First, prevent successful attacks by decreasing intrusion rates, establishing security layers, training for cyber-awareness, etc. We know that to allocate resources we need more detail for these types of recommendations, because the defensive costs for cyber are higher

than to attack opponent. Analytical and numerical examples show that defensive actions may be more effective than offensive actions in cyber operations. We provide tools to compare and analyze these tradeoffs.

For instance, it is better to conduct five intrusions, each infecting one unit in the adversary system in different times, than it is to conduct one intrusion and infect five units at that time, assuming that all are using the same infection.

Secondly, keeping a high fraction of the force in the recovered state is as important as having a high patch rate. If a force can keep the cyber security of its units updated, the starting conditions will be in favor of the defender, and the cyber attack can be stopped before it becomes a pandemic.

These insights may differ for specific zero day vulnerabilities. For cases in which the attacker takes the risk of being intercepted, it may be better to wait to for a promising level of infected units or for the discovery of a defender vulnerability to launch a cyber attack. The above phenomenon is not currently captured in the models, but is a strong candidate for future work

C. FURTHER RESEARCH

We are at the very beginning of modeling coordinated cyber and kinetic phenomena. Academic literature on this topic is still fairly young. Since there are various ways to use and extend the models in this study, we have started from basics. In this context, future work can be focused on exploring proposed extensions, or adopting different infection spread systems. A more detailed study is needed to explore other types of cyber attacks. Adding stochasticity to studied models and validating proposed models with real world data are two main courses for further research.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX A. DEFINITION OF TERMS

These are the term definitions published, or commonly accepted, and generally used with the same meaning outside of this study. We refer to military documents regarding the purpose of the study.

Navigation warfare: Deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare operations. Also called NAVWAR. (JP-3-14)

Offensive cyberspace operations: Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called OCO. (JP 3–12)

Cyber Capability: Any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities. Cyber capabilities do not include a device or software that is solely intended to provide access to an adversarial computer system for data exploitation. (AFI 51–402)

Cyberspace Operations: A cyberspace operation is the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (AFI 51–402)

Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (Joint Pub 3–13)

Cyber (adj.): Of or pertaining to the cyberspace environment, capabilities, plans, or operations. (Air Force definition)

Cyber Capability: Any device or software payload intended to disrupt, deny, degrade, negate, impair, or destroy adversarial computer systems, data, activities, or capabilities. Cyber capabilities do not include a device or software that is solely intended to provide access to an adversarial computer system for data exploitation. (AFI 51–402)

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Joint Pub 1–02)

Cyberspace Operations: The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. (Joint Pub 3–0)

Cyberspace Superiority: The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference. (AFDD 3–12)

Cyberspace Support: Foundational, continuous, or responsive operations in order to ensure information integrity and availability in, through, or from Air Force controlled infrastructure and its interconnected analog and digital portion of the battle space. (AFDD 3–12)

Defensive Cyberspace Operations (DCO): DCO direct and synchronize actions to detect, analyze, counter, and mitigate cyber threats and vulnerabilities; outmaneuver adversaries taking or about to take offensive actions; and otherwise protect critical missions that enable our freedom of action in cyberspace. (USCYBERCOM Concept of Operations, v 1.0, 21 Sep 2010)

Defensive Cyberspace Operations (DCO): DCO direct and synchronize actions to detect, analyze, counter, and mitigate cyber threats and vulnerabilities; outmaneuver adversaries taking or about to take offensive actions; and otherwise protect critical missions that enable our freedom of action in cyberspace. (USCYBERCOM Concept of Operations, v 1.0, 21 Sep 2010)

Global Information Grid (GIG): The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. (Joint Pub 6–0)

Information Assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (AFPD 33–2, Joint Pub 3–13)

Information Superiority: The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Pub 3–13)

Offensive Cyberspace Operations (OCO): The creation of various enabling and attack effects in cyberspace, to meet or support national and combatant commanders' objectives and actively defend DOD or other information networks, as directed. (USCYBERCOM Concept of Operations, v 1.0, 21 Sep 2010)

APPENDIX B. MODEL ENVIRONMENT

In this section, we describe the terms and the concept of cyber operations. Although these types of operations widely vary by nature, we use the most general form and explain the cyber warfare by phases agreed upon.

Asymmetric Threat

According to the DOD *Dictionary of Military and Associated Terms* (JP1-02), asymmetric means: "In military operations the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent's strengths while exploiting his weaknesses." The term asymmetric threat is used when the threat has the potential to cause damage at an extraordinary ratio to its effort. Effort can be quantified by its cost, information requirement, manpower, access to resources etc. In those terms, terrorist attacks like suicide bombs, IED/mine threats, guerilla attacks are types of asymmetric threats.

We can categorize cyber threat as an asymmetric threat, because of its impact regarding its effort. In cyberspace, even one person with proper skills and interest can become a national threat. It is easy to cause a national disaster with an organized cyber attempt. When this effect is joined with kinetic effects in battle, its multiplicative effect will boost the attacking force.

Cyber Environment

Anything related to electronic devices can be affected by cyber operations. In other words, we would be immune to a cyber operation if we were to use a bow to hunt, and only use candle light at night. But, as was stated before, anything electronic or related to electronics can be affected by a cyber operation.

Cyber Forces

A cyber operation typically consists of the following elements:

- Specific equipment: Such as computers, data connectors, input devices.
- Specialized personnel: At least one person with knowledge and training about cyber operations. This person can write autonomous programs, which

are able to work independently, but we need a code-writer before that code copies itself.

- Physical contact: Even with specific equipment and specialized personnel, we may not be able to conduct a cyber operation. We may need a physical contact with the target network and special equipment. All data transfer assets including electromagnetic spectrum and supply chain intrusion can provide this contact.

We assume these three requirements are physical necessities.

We can categorize the cyber operational forces into two groups as Human Controlled Program (HCP) and Automated Program (AP). Both these groups need to satisfy physical requirements and are categorized by working process. We use APs in this study as a cyber threat, because it is more commonly used in larger cyber environments, and HCP works like the APs in the beginning. HCP is used in cyber operations for special units, which is not in our focus in this study. We ignore human-related concerns behind APs, such as training level or communication skill, and just focus on the product AP, as it can work independently.

Non-combatant units, units which do not have any offensive or defensive assets, can be categorized as white population. But, even white units can be controlled with any of the fighting forces without approval (or notice) of the white user, and can be used as a reserve.

Cyber Weapons

Cyber weapons are special programs *(tools)* used as weapons in cyberspace. A human may or may not be necessary to use this tool, meaning that tools can be trigger activated, or pre-programmed, or use basic artificial intelligence. Also, any program can be equipped with disguised tools and can be weaponized.

Objectives of Cyber Operations

After regulations made in 2010 concerning cyber forces (Lynn, 2010), we assume that the cyber domain is another front in a kinetic combat, one which requires strategy, resources and tactics. Although cyber operations may have a variety of objectives, such as stealing information, locking data (ransomware), changing data, destroying data, slowing

down communications, slowing down systems and information propagation, etc., we focus on slowing down communications and/or system operations.

Phases of Cyber Operations

We can generalize the cyber operation phases by using the attack phases. The sequence of an attack process is

- Recon,
- Scan,
- Access,
- Escalate,
- Exfiltrate,
- Assault,
- Sustain, and
- Obfuscate.(Winterfeld and Andress, 2012).

Tasks of Cyber Operations

Cyber operations can be tasked in various ways. These operations may be limited to cyber space, as well as extending to physical environments. A cyber force can do each of the tasks below to critical data or software, which indirectly affects adversary. Also, these tasks can be used for direct attacks in order to shut down electric sources and grids, communication lines, production assets, disrupt or change control measurements to cause a critical or fatal fault on mechanical or even nuclear parts etc…

Programs can execute tasks such as:

- Attack,
- Block,
- Delay,
- Disrupt,
- Destroy,
- Isolate,
- Screen, and
- Withdraw.

Types of Cyber Attacks

Cyber attacks can be categorized in two main parts: Logical cyber attacks and Physical cyber attacks (Andress and Winterfeld, 2013).

Logical cyber attacks use:

- Recon tools,
- Scan tools,
- Access and escalation tools,
- Exfiltration tools,
- Assault tools, and
- Obfuscation tools.

Physical cyber attacks use:

- Supply chain attack tools, and
- SCADA (Infrastructure) attack tools.

Each type of attack uses different attributes of cyber environments, and should be modeled separately. So we introduce different models for different attack types.

In our models, we use the fact that the effect of a cyber attack starts with the Access phase. Recon – Scan phases just supply intelligence for further phases. Also, the damage happens in the Assault phase, where the action happens. The Escalate phase expands the reach of attack as much as possible, whereas the Exfiltrate phase limits the reach in order to adjust the focus on the right target. Sustain – Obfuscate phases are about erasing any trails to prevent backtrack.

In order to model a realistic scenario, we can simplify these phases into three as: **Access, Escalate** and **Assault**. In this case we assume that Recon and Scan phases were completed before, and we assume no evidence of the phases remains..

In this context, for any type of cyber attacks (including web defacement attacks, DOS attacks, zero-day attacks, malicious code attacks…) for a closed network as a military network, malicious code needs to be used for access, escalate, or assault phases. We use epidemiology to model cyber infection for these three phases.

APPENDIX C. EXPLORING EPIDEMIC COMBAT MODEL

1. Steps to Dynamic State Equations

The original equations from Schramm and Gaver (2013), as a one-sided model specified in (4.1) - (4.4):

$$\frac{dZ}{dt} = -\beta_U(S+R) - \beta_D\,(I)\,,$$

$$\frac{dS}{dt} = (-\xi\,S\,I - \eta\,S\,R) - \rho\,Z\,\frac{S}{S+I+R}\,,$$

$$\frac{dI}{dt} = (\xi\,I\,S - \eta\,I\,R) - \rho\,Z\,\frac{I}{S+I+R}\,,$$

$$\frac{dR}{dt} = (\eta\,S\,R + \eta\,R\,I) - \rho\,Z\,\frac{R}{S+I+R}\,.$$

We modify this one sided model to two sided by adding the cyber effect to both sides numerically as in (4.5) - (4.10):

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B - \eta_B S_B R_B) - [\rho_U(S_Z+R_Z) + \rho_D\,(I_Z)]\,\frac{S_B}{S_B+I_B+R_B}$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \eta_B I_B R_B) - [\rho_U(S_Z+R_Z) + \rho_D\,(I_Z)]\,\frac{I_B}{S_B+I_B+R_B}$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B) - [\rho_U(S_Z+R_Z) + \rho_D\,(I_Z)]\,\frac{R_B}{S_B+I_B+R_B}$$

$$\frac{dS_Z}{dt} = (-\xi_Z S_Z I_Z - \eta_Z S_Z R_Z) - [\,\beta_U(S_B+R_B) + \beta_D\,(I_B)]\,\frac{S_z}{S_Z+I_Z+R_Z}$$

$$\frac{dI_Z}{dt} = (+\xi_Z I_Z\,S_Z - \eta_Z I_Z\,R_Z) - [\,\beta_U(S_B+R_B) + \beta_D\,(I_B)]\,\frac{I_z}{S_Z+I_Z+R_Z}$$

$$\frac{dR_Z}{dt} = (+\eta_Z R_Z S_Z + \eta_Z R_Z I_Z) - [\,\beta_U(S_B+R_B) + \beta_D\,(I_B)]\,\frac{R_z}{S_Z+I_Z+R_Z}$$

We define in Section IV.A that

$$S_B + I_B + R_B = B$$

$$S_Z + I_Z + R_Z = Z$$

We define in (4.11) and (4.12) that:

$$\frac{\mathrm{d}B}{\mathrm{d}t} = -\rho_U(S_Z + R_Z) - \rho_D\,(I_Z)\,,$$

$$\frac{\mathrm{d}Z}{\mathrm{d}t} = -\beta_U(S_B + R_B) - \beta_D\,(I_B)\,,$$

We define in (4.21) and (4.22) that:

$$\frac{\mathrm{d}B}{\mathrm{d}t} = -\bar{\rho}\,Z\ ,$$

$$\frac{\mathrm{d}Z}{\mathrm{d}t} = -\bar{\beta}\,B\ ,$$

A more compact form is represented as:

$$\frac{\mathrm{d}S_B}{\mathrm{d}t} = (-\xi_B S_B I_B - \eta_B S_B R_B) - \bar{\rho}\,Z\,\frac{S_B}{B},$$

$$\frac{\mathrm{d}I_B}{\mathrm{d}t} = (+\xi_B I_B S_B - \eta_B I_B R_B) - \bar{\rho}\,Z\,\frac{I_B}{B},$$

$$\frac{\mathrm{d}R_B}{\mathrm{d}t} = (+\eta_B R_B S_B + \eta_B R_B I_B) - \bar{\rho}\,Z\frac{R_B}{B}\,,$$

$$\frac{\mathrm{d}S_Z}{\mathrm{d}t} = (-\xi_Z S_Z I_Z - \eta_Z S_Z R_Z) - \bar{\beta}\,B\ \ \frac{S_z}{Z}\,,$$

$$\frac{\mathrm{d}I_Z}{\mathrm{d}t} = (+\xi_Z I_Z\,S_Z - \eta_Z I_Z\,R_Z) - \bar{\beta}\,B\ \ \frac{I_z}{Z}\,,$$

$$\frac{\mathrm{d}R_Z}{\mathrm{d}t} = (+\eta_Z R_Z S_Z + \eta_Z R_Z I_Z) - \bar{\beta}\,B\ \ \frac{R_z}{Z}\,.$$

We use the form as in (4.13) - (4.18) to manipulate the equations on one side:

$$\frac{\mathrm{d}S_B}{\mathrm{d}t} = (-\xi_B S_B I_B - \eta_B S_B R_B) + \frac{\mathrm{d}B}{\mathrm{d}t}\frac{S_B}{B},$$

$$\frac{\mathrm{d}I_B}{\mathrm{d}t} = (+\xi_B I_B S_B - \eta_B I_B R_B) + \frac{\mathrm{d}B}{\mathrm{d}t}\frac{I_B}{B},$$

$$\frac{\mathrm{d}R_B}{\mathrm{d}t} = (+\eta_B R_B S_B + \eta_B R_B I_B) + \frac{\mathrm{d}B}{\mathrm{d}t}\frac{R_B}{B},$$

$$\frac{\mathrm{d}S_Z}{\mathrm{d}t} = (-\xi_Z S_Z I_Z - \eta_Z S_Z R_Z) + \frac{\mathrm{d}Z}{\mathrm{d}t}\frac{S_z}{Z},$$

$$\frac{\mathrm{d}I_Z}{\mathrm{d}t} = (+\xi_Z I_Z S_Z - \eta_Z I_Z R_Z) + \frac{\mathrm{d}Z}{\mathrm{d}t}\frac{I_z}{Z},$$

$$\frac{\mathrm{d}R_Z}{\mathrm{d}t} = (+\eta_Z R_Z S_Z + \eta_Z R_Z I_Z) + \frac{\mathrm{d}Z}{\mathrm{d}t}\frac{R_z}{Z}.$$

A reduced system of equations for the Blue side,

$$\frac{dS_B}{dt} = (-\xi_B S_B I_B - \eta_B S_B R_B) + \frac{dB}{dt}\frac{S_B}{B},$$

$$\frac{dI_B}{dt} = (+\xi_B I_B S_B - \eta_B I_B R_B) + \frac{dB}{dt}\frac{I_B}{B},$$

$$\frac{dR_B}{dt} = (+\eta_B R_B S_B + \eta_B R_B I_B) + \frac{dB}{dt}\frac{R_B}{B}.$$

Note that from here we refer to initial states of Blue with representation (S_0, I_0, R_0). These equations are not equivalent to six equations in (4.5) - (4.10).

From these derive equations as:

$$\frac{1}{S_B}dS_B - \frac{1}{B}dB = (-\xi_B I_B - \eta_B R_B)\ dt \qquad (5.37)$$

$$\frac{1}{I_B}dI_B - \frac{1}{B}dB = (+\xi_B S_B - \eta_B R_B)\ dt \qquad (5.38)$$

$$\frac{1}{R_B}dR_B - \frac{1}{B}dB = (+\eta_B S_B + \eta_B I_B)\ dt \qquad (5.39)$$

By subtracting (5.38) from (5.37) :

$$\frac{1}{S_B} dS_B - \frac{1}{I_B} dI_B = -\xi_B (I_B + S_B)\ dt \qquad (5.40)$$

By writing (5.39) in the same form:

$$\frac{1}{R_B} dR_B - \frac{1}{B} dB = +\eta_B (S_B + I_B)\ dt \qquad (5.41)$$

By dividing (5.40) by (5.41):

$$\frac{\frac{1}{S_B} dS_B - \frac{1}{I_B} dI_B}{\frac{1}{R_B} dR_B - \frac{1}{B} dB} = \frac{-\xi_B\ (I_B + S_B)\ dt}{+\eta_B\ (S_B + I_B)\ dt}$$

After cancellations on each side:

$$\frac{1}{S_B} dS_B - \frac{1}{I_B} dI_B = -\frac{\xi_B}{\eta_B} (\frac{1}{R_B} dR_B - \frac{1}{B} dB) \qquad (5.42)$$

By integrating both sides in (5.42), we derive the equation:

$$ln(\frac{S_B}{I_B}) - \ ln(\frac{S_0}{I_0}) = -\frac{\xi_B}{\eta_B} (ln(\frac{R_B}{B}) - ln(\frac{R_0}{B_0}))$$

Which leads to:

$$-ln(\frac{\frac{S_B}{I_B}}{\frac{S_0}{I_0}}) = \frac{\xi_B}{\eta_B} (ln(\frac{\frac{R_B}{B}}{\frac{R_0}{B_0}}))$$

We modify the equation as:

$$ln\left(\frac{\frac{S_B}{I_B}}{\frac{S_0}{I_0}}\right)^{-1} = ln\left(\frac{\frac{R_B}{B}}{\frac{R_0}{B_0}}\right)^{\frac{\xi_B}{\eta_B}}$$

We can simplify the equation for Blue as:

$$\frac{\frac{I_B}{I_0}}{\frac{S_B}{S_0}} = \left(\frac{\frac{R_B}{R_0}}{\frac{B}{B_0}}\right)^{\xi/\eta} \qquad (5.43)$$

For $S_B, I_B, R_B > 0$, the dynamic state equation in two different representations as:

$$\left(\frac{B}{B_0}\right)^{\xi/\eta} \frac{I_B}{I_0} = \left(\frac{R_B}{R_0}\right)^{\xi/\eta} \frac{S_B}{S_0}\,, \qquad (5.44)$$

$$R_B\left(\frac{S_B}{I_B}\right)^{\eta/\xi} = c\,B, \qquad c = \frac{R_0}{B_0}\left(\frac{S_0}{I_0}\right)^{\eta/\xi} \qquad (5.45)$$

Note that all initial states S_0, I_0, R_0, parameters ξ, η belong to *B*, and c is constant. These calculations were represented for Blue side only, but can be calculated for Red side, also.

Consider the case for "no kinetic battle" or "no attrition" and spread rate equals to patch rate. In that case, $\frac{B}{B_0}$ is 1 and $\xi = \eta$. These assumptions will lead the equation to:

$$\frac{I_B}{I_0} = \left(\frac{R_B}{R_0}\right)\frac{S_B}{S_0}$$

which is a different representation of Schramm and Gaver (2013) for closed form of *I(t)*, which uses the same assumptions.

D. Approximation Calculations to Estimate Cyber Operation Value

1. Scaled Cyber Time – Kinetic Combat Time

We used the equations $\bar{\beta} = \beta_U - I_B^{\alpha}(\beta_U - \beta_D)$ and $\bar{\rho} = \rho_U - I_Z^{\alpha}(\rho_U - \rho_D)$ for variable attack rates. Figure 26 shows how the attack rates may change by time when cyber effects are considered. Using these rates as functions of time will give us the exact solution, but give us a hard time to solve for. To simplify the process, we can approximate the result by using a constant average number of attack rates. Note that using a constant average attack rate instead of calculating whole process may be misleading, because we simply ignore the variability of the process and try to overcome a dynamic process by using two constant numbers. However, if there is enough data for the effects of these rates, using average numbers can be safer, and will allow us to implement different types of dynamic models into large simulation models, which are used in military decision making.

Here we show a notional simplified example by comparing two battles; in Figure 39 both sides have cyber capabilities, and one side (Blue) is using kinetic attack, affected dynamically, and in Figure 40 we model the same battle with a constant kinetic attack rate. Note that changing the parameters will change the situation, and the constant attack rate should be re-evaluated. These average attack rates will approximate to real battle results, but a systematic way to estimate the average constant attack rate is beyond the scope of this study.

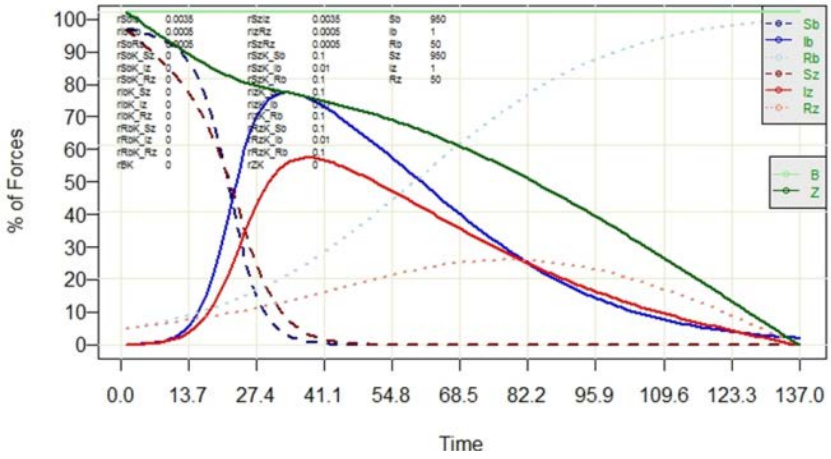

Figure 39. Force levels in numerical experiment ($\beta_U = 0.1, \beta_D = 0.01$)

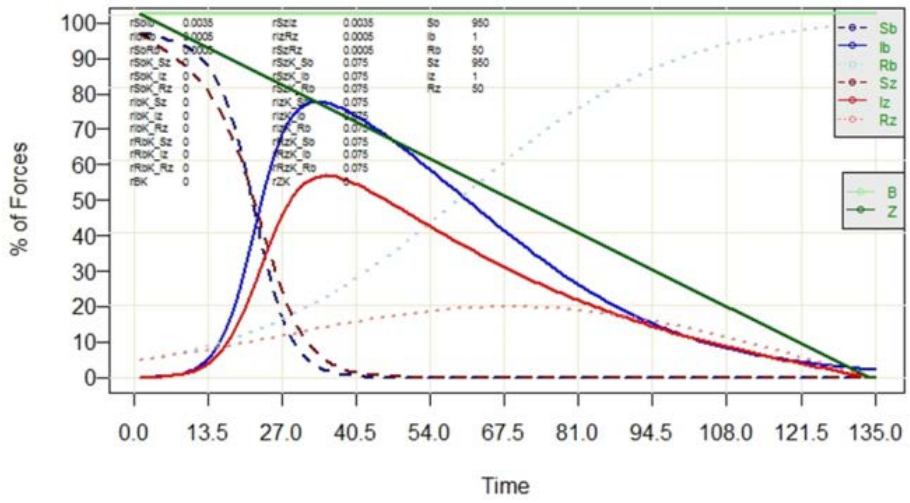

Figure 40. Force levels in using average approximation ($\bar{\beta} = 0.075$)

2. Different Types of Models

We used epidemic models and kinetic combat models and combined them to explain the effect of cyber operations. It is important to point out that the infection term in epidemic model was used to demonstrate cyber effects in a battle in this study, but in fact this term can be used in different ways.

The term **"Infection"** used in this study is a broad term which can be used for any effect that reduces a force's warfighting capabilities. The scope of examples can be as broad as, propaganda via media which affects a force psychologically, chemical or biological weapons which affects a force biologically, terror actions which damage infrastructure etc.; basically all kinds of asymmetric threats. The scenario in this thesis considers malware infection on electronic devices, but the model can be used in much broader cases.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, J. 2013. March 2000, Testimony of James Adams, Chief Executive Officer Infrastructure Defense, Inc. to Committee on Governmental Affairs United States Senate. http://www.hsgac.senate.gov/download/?id=57137fee-272b-4700-afb2-302231a11d81. Accessed March 11 .

Andress, J., S. Winterfeld. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (2nd ed.). Syngress Publishing, Waltham, MA.

Chen, Z., C. Chen. 2008. Deriving a closed-form expression for worm-scanning strategies. *International Journal of Security and Networks*, *4*(3), 135–144.

Cigital. 2013. President Obama Acknowledges Cyber Threat and Signs Executive Order for Improving Critical Infrastructure Cybersecurity. Cigital Online. http://www.cigital.com/justice-league-blog/2013/02/13/president-obama-acknowledges-cyber-threat-and-signs-executive-order/.

Decker, B., W. C. Douglass, II. 2011. *Bowing to Beijing: How Barack Obama Is Hastening America's Decline and Ushering ina Century of Chinese Domination*. Regnery Publishing, Washington, DC.

Defense Science Board. 2013.Task Force Report: Resilient Military Systems Cyber Threat,http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf (October 10).

The Economist. 2010. Cyberwar: War in the fifth domain. *The Economist*. Online edition (July 1).

Engel, J. H., 1954. A verification of Lanchester's law. *Journal of the Operations Research Society of America* **2** 163–171.

Gonsalves, A. 2012. Bank attackers more sophisticated than typical hacktivists, expert says. CSO Online - Security and Risk. http://www.csoonline.com/article/2132319/malware-cybercrime/bank-attackers-more-sophisticated-than-typical-hacktivists--expert-says.html

Grant, R. 1999. Airpower made it work. *Air Force Magazine* **82** 30–37.

Hancock, B. 1999. Security view. *Comput. Secur.* **18** 553–564.

Hartley, D. S. 2001. *Predicting combat effects*, 1, *INFORMS, Linthicum Md* (2001).

Ihaka, R., & Gentleman, R. (1996). R: a language for data analysis and graphics. *Journal of computational and graphical statistics*, *5*(3), 299–314.

Jones, J. H. (2007). Notes on R0. *Department of Anthropological Sciences Stanford University*. http://www.stanford.edu/~jhj1/teachingdocs/Jones-on-R0.pdf

Kermack, W., A. McKendrick. 1927. Contributions to the mathematical theory of epidemics—I. *Bulletin of Mathematical Biology* (1991) **53**(1–2), 33–55.

Lanchester, F. W. 1916. *Aircraft in warfare: the dawn of the fourth arm*. Constable limited, Appleton, NY.

Lucas, T. W. 2000. The stochastic versus deterministic argument for combat simulations: Tales of when the average won't do. *Mil. Oper. Res.* **5,** 9–28.

Lynn, W. J., III. 2010. Defending a new domain. *Foreign Affairs* **89,** 97–108.

McMorrow, D. *Science of Cyber-Security*. No. JSR-10-102. Mitre Corp, Mclean, VA, Jason Program Office, 2010. DTIC Document.

Murray, J. D. 2002. Mathematical Biology I: An Introduction, vol. 17 of Interdisciplinary Applied Mathematics. Springer, New York, NY.

Nakashima, E. 2013. Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. *The Washington Post*. Online edition (May 27).

Newman, M. E. 2002. Spread of epidemic disease on networks. *Phys. Rev. E.* **66**, 016128.

Obama, B. 2013. Executive Order–Improving Critical Infrastructure Cybersecurity. The White House, Washington, DC.

Sanger, D. E. 2012. Obama order speeds up wave of cyberattacks against Iran. *New York Times*. Online edition (July 1).

Schramm, Harrison C. "Lanchester models with discontinuities: An application to networked forces." *Mil. Oper. Res.* 17.4 (2012), 59–68.

Schramm, H. C., & Gaver, D. P. (2013). Lanchester for cyber: The mixed epidemic combat model. *Naval Research Logistics (NRL)*, 60(7), 599–605.

Shamah, D. 2013. Cyber espionage bug attacking Middle East but Israel untouched so far. *The Times of Israel*. Online edition (June 4).

Singel, B. 2010. White House cyber czar: There is no cyberwar. *Wired Magazine*. Online edition (March 4).

Soetaert, K., T. Petzoldt, R. W. Setzer. 2010. Solving differential equations in R: Package deSolve. *J. of Statistical Software* **33** 1–25.

Sommer, P. 2011. Reducing Systemic Cybersecurity Risk. OECD Multi-Displinary Issues.

Symantec, 2012, Internet Security Threat Report 2011, *Symantec Online*, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (April).

Symantec, 2014, Internet Security Threat Report 2013, Symantec Online, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (April).

U.S. Department of Defense. 2009. Annual Report to Congress, Military Power of the People's Republic of China, 22.

U.S. Department of Defense. 2011. DOD Strategy for Operating in Cyberspace.

Van Mieghem, P., J. Omic, R. Kooij. 2009. Virus spread in networks. *IEEE/ACM Transactions on Networking* **17(1),** 1–14.

Vojnovic, M., A. J. Ganesh. 2008. On the race of worms, alerts, and patches. *IEEE/ACM Transactions on Networking* **16(5)**, 1066–1079.

Washburn, A., M. Kress. 2009. *Combat Modeling*. Springer, New York.

The White House. 2009. *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. The White House, Washington, DC.

Wiener, Norbert. *Cybernetics or Control and Communication in the Animal and the Machine*, vol. 25. MIT press, 1965.

Winterfeld, S., J. Andress. 2012. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Newnes, Boston, MA.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California